

# P-2812HNU(L)-Fx Series

802.11n Wireless VDSL2 VoIP Combo WAN IAD

## User's Guide



### Default Login Details

IP Address	http://192.168.1.1
User Name	Admin account: admin User account: user
Password	Admin account: 1234 User account: 1234

Firmware Version 3.10  
Edition 1, 3/2011

[www.zyxel.com](http://www.zyxel.com)

# ZyXEL



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the Device using the web configurator.

## Tips for Reading User's Guides On-Screen

When reading a ZyXEL User's Guide On-Screen, keep the following in mind:

- If you don't already have the latest version of Adobe Reader, you can download it from <http://www.adobe.com>.
- Use the PDF's bookmarks to quickly navigate to the areas that interest you. Adobe Reader's bookmarks pane opens by default in all ZyXEL User's Guide PDFs.
- If you know the page number or know vaguely which page-range you want to view, you can enter a number in the toolbar in Reader, then press [ENTER] to jump directly to that page.
- Type [CTRL]+[F] to open the Adobe Reader search utility and enter a word or phrase. This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader.
- To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen.
- Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF.

## Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

## Documentation Feedback

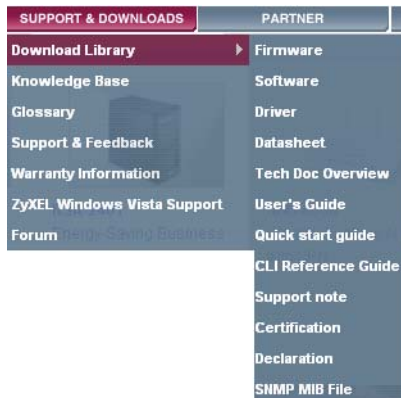
Send your comments, questions or suggestions to: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,  
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

## Need More Help?

More help is available at [www.zyxel.com](http://www.zyxel.com).



- **Download Library**

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- **Knowledge Base**

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- **Forum**

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

## Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See [http://www.zyxel.com/web/contact\\_us.php](http://www.zyxel.com/web/contact_us.php) for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.



# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

**Warnings tell you about things that could harm you or your device.**




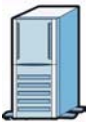
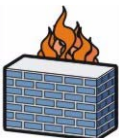



Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

## Syntax Conventions

- The P-2812HNU(L)-Fx Series may be referred to as the "Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

## Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The Device icon is not an exact representation of your device.

Device 	Computer 	Notebook computer 
Server 	Firewall 	Telephone 
Router 	Switch 	

# Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- This product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.





# Contents Overview

<b>User's Guide .....</b>	<b>19</b>
Introduction .....	21
Introducing the Web Configurator .....	27
Tutorials .....	33
<b>Technical Reference .....</b>	<b>79</b>
Connection Status and System Info .....	81
Broadband .....	87
Wireless .....	123
Home Networking .....	149
Routing .....	173
Quality of Service (QoS) .....	177
Network Address Translation (NAT) .....	189
Dynamic DNS .....	197
Firewall .....	199
MAC Filter .....	205
Parental Control .....	207
Certificates .....	211
VoIP .....	219
Logs .....	243
Traffic Status .....	247
User Account .....	253
Remote MGMT .....	255
System .....	257
Time Setting .....	259
Log Setting .....	261
Firmware Upgrade .....	263
Backup/Restore .....	265
Diagnostic .....	269
Troubleshooting .....	273
Product Specifications .....	281



# Table of Contents

<b>About This User's Guide .....</b>	<b>3</b>
<b>Document Conventions .....</b>	<b>5</b>
<b>Safety Warnings.....</b>	<b>7</b>
<b>Contents Overview .....</b>	<b>9</b>
<b>Table of Contents .....</b>	<b>11</b>
 <b>Part I: User's Guide .....</b>	 <b>19</b>
<b>Chapter 1</b>	
<b>Introduction.....</b>	<b>21</b>
1.1 Overview .....	21
1.2 Applications for the Device .....	21
1.2.1 Internet Access .....	21
1.2.2 VoIP Features .....	22
1.2.3 Wireless Connection .....	22
1.3 The WLAN Button .....	23
1.4 Ways to Manage the Device .....	24
1.5 Good Habits for Managing the Device .....	24
1.6 LEDs (Lights) .....	24
1.7 The RESET Button .....	26
 <b>Chapter 2</b>	
<b>Introducing the Web Configurator .....</b>	<b>27</b>
2.1 Overview .....	27
2.1.1 Accessing the Web Configurator .....	27
2.2 The Web Configurator Layout .....	29
2.2.1 Title Bar .....	29
2.2.2 Main Window .....	29
2.2.3 Navigation Panel .....	30
 <b>Chapter 3</b>	
<b>Tutorials.....</b>	<b>33</b>
3.1 Overview .....	33
3.2 Setting Up Your DSL Connection .....	33
3.3 How to Set up a Wireless Network .....	36

3.3.1 Example Parameters .....	36
3.3.2 Configuring the AP .....	36
3.3.3 Configuring the Wireless Client .....	38
3.4 Setting Up NAT Port Forwarding .....	43
3.5 How to Make a VoIP Call .....	44
3.5.1 VoIP Calls With a Registered SIP Account .....	45
3.6 Using the File Sharing Feature .....	47
3.6.1 Set Up File Sharing .....	48
3.6.2 Access Your Shared Files From a Computer .....	49
3.7 Using the Media Server Feature .....	49
3.7.1 Configuring the Device .....	50
3.7.2 Using Windows Media Player .....	50
3.7.3 Using a Digital Media Adapter .....	53
3.8 Using the Print Server Feature .....	55
3.9 Configuring the MAC Address Filter .....	70
3.10 Configuring Static Route for Routing to Another Network .....	71
3.11 Configuring QoS Queue and Class Setup .....	73
3.12 Access the Device Using DDNS .....	76
3.12.1 Registering a DDNS Account on <a href="http://www.dyndns.org">www.dyndns.org</a> .....	77
3.12.2 Configuring DDNS on Your Device .....	77
3.12.3 Testing the DDNS Setting .....	77

## **Part II: Technical Reference.....79**

### **Chapter 4**

#### **Connection Status and System Info ..... 81**

4.1 Overview .....	81
4.2 The Connection Status Screen .....	81
4.3 The System Info Screen .....	83

### **Chapter 5**

#### **Broadband..... 87**

5.1 Overview .....	87
5.1.1 What You Can Do in this Chapter .....	88
5.1.2 What You Need to Know .....	88
5.1.3 Before You Begin .....	91
5.2 The Broadband Screen .....	91
5.2.1 Add/Edit Internet Connection .....	93
5.3 The 3G Backup Screen .....	115
5.4 Technical Reference .....	117



<b>Chapter 6</b>	
<b>Wireless .....</b>	<b>123</b>
6.1 Overview .....	123
6.1.1 What You Can Do in this Chapter .....	123
6.1.2 Wireless Network Overview .....	123
6.1.3 Before You Begin .....	125
6.2 The Wireless General Screen .....	125
6.2.1 No Security .....	127
6.2.2 Basic (Static WEP/Shared WEP Encryption) .....	127
6.2.3 More Secure (WPA(2)-PSK) .....	129
6.2.4 WPA(2) Authentication .....	130
6.3 The More AP Screen .....	131
6.3.1 Edit More AP .....	132
6.4 The WPS Screen .....	133
6.5 The WMM Screen .....	135
6.6 Scheduling Screen .....	137
6.7 Technical Reference .....	137
6.7.1 Additional Wireless Terms .....	138
6.7.2 Wireless Security Overview .....	138
6.7.3 Signal Problems .....	140
6.7.4 BSS .....	141
6.7.5 MBSSID .....	141
6.7.6 WiFi Protected Setup (WPS) .....	142
<b>Chapter 7</b>	
<b>Home Networking .....</b>	<b>149</b>
7.1 Overview .....	149
7.1.1 What You Can Do in this Chapter .....	149
7.1.2 What You Need To Know .....	149
7.2 The LAN Setup Screen .....	152
7.3 The Static DHCP Screen .....	153
7.3.1 Before You Begin .....	153
7.4 The UPnP Screen .....	155
7.5 The File Sharing Screen .....	155
7.5.1 Before You Begin .....	156
7.5.2 Add/Edit File Sharing .....	157
7.6 The Media Server Screen .....	158
7.7 The Printer Server Screen .....	159
7.7.1 Before You Begin .....	159
7.8 Technical Reference .....	160
7.9 Installing UPnP in Windows Example .....	164
7.10 Using UPnP in Windows XP Example .....	167

<b>Chapter 8</b>	
<b>Routing .....</b>	<b>173</b>
8.1 Overview .....	173
8.2 Configuring Static Route .....	174
8.2.1 Add/Edit Static Route .....	175
<b>Chapter 9</b>	
<b>Quality of Service (QoS).....</b>	<b>177</b>
9.1 Overview .....	177
9.1.1 What You Can Do in this Chapter .....	177
9.1.2 What You Need to Know .....	177
9.2 The QoS General Screen .....	178
9.3 The Queue Setup Screen .....	180
9.3.1 Add/Edit a QoS Queue .....	181
9.4 The Class Setup Screen .....	181
9.4.1 Add/Edit QoS Class .....	183
9.5 The QoS Monitor Screen .....	186
9.6 QoS Technical Reference .....	187
9.6.1 IEEE 802.1Q Tag .....	187
9.6.2 IP Precedence .....	187
9.6.3 DiffServ .....	187
<b>Chapter 10</b>	
<b>Network Address Translation (NAT).....</b>	<b>189</b>
10.1 Overview .....	189
10.1.1 What You Can Do in this Chapter .....	189
10.1.2 What You Need To Know .....	189
10.2 The Port Forwarding Screen .....	190
10.2.1 The Port Forwarding Screen .....	190
10.2.2 The Port Forwarding Edit Screen .....	192
10.3 The Sessions Screen .....	193
10.4 Technical Reference .....	193
10.4.1 NAT Definitions .....	193
10.4.2 What NAT Does .....	194
10.4.3 How NAT Works .....	194
<b>Chapter 11</b>	
<b>Dynamic DNS .....</b>	<b>197</b>
11.1 Overview .....	197
11.1.1 What You Need To Know .....	197
11.2 The Dynamic DNS Screen .....	197

<b>Chapter 12</b>	
<b>Firewall</b>	<b>199</b>
12.1 Overview	199
12.1.1 What You Can Do in this Chapter	199
12.1.2 What You Need to Know	199
12.2 The General Screen	200
12.3 The Services Screen	201
12.4 Firewall Technical Reference	202
12.4.1 Guidelines For Enhancing Security With Your Firewall	202
12.4.2 Security Considerations	202
<b>Chapter 13</b>	
<b>MAC Filter</b>	<b>205</b>
13.1 Overview	205
13.1.1 What You Need to Know	205
13.2 The MAC Filter Screen	205
<b>Chapter 14</b>	
<b>Parental Control</b>	<b>207</b>
14.1 Overview	207
14.2 The Parental Control Screen	207
14.2.1 Add/Edit a Parental Control Rule	208
<b>Chapter 15</b>	
<b>Certificates</b>	<b>211</b>
15.1 Overview	211
15.1.1 What You Can Do in this Chapter	211
15.1.2 What You Need to Know	211
15.1.3 Verifying a Certificate	212
15.2 Local Certificates	213
15.3 Trusted CA	215
15.4 Trusted CA Import	215
15.5 View Certificate	216
<b>Chapter 16</b>	
<b>VoIP</b>	<b>219</b>
16.1 Overview	219
16.1.1 What You Can Do in this Chapter	219
16.1.2 What You Need to Know	219
16.1.3 Before You Begin	221
16.2 The SIP Service Provider Screen	221
16.3 The SIP Account Screen	224
16.3.1 Add/Edit SIP Account	226

16.4 Multiple SIP Accounts .....	228
16.5 The Common Screen .....	228
16.6 Phone Screen .....	229
16.6.1 Edit Phone Device .....	230
16.7 The Phone Region Screen .....	231
16.8 The Call Rule Screen .....	231
16.9 The FXO Screen ("L" Models Only) .....	233
16.10 Technical Reference .....	233
16.10.1 VoIP .....	234
16.10.2 SIP .....	234
16.10.3 Quality of Service (QoS) .....	238
16.10.4 Phone Services Overview .....	239
<b>Chapter 17</b>	
<b>Logs .....</b>	<b>243</b>
17.1 Overview .....	243
17.1.1 What You Can Do in this Chapter .....	243
17.1.2 What You Need To Know .....	243
17.2 The System Log Screen .....	244
17.3 The Phone Log Screen .....	245
17.4 The VoIP Call History Screen .....	245
<b>Chapter 18</b>	
<b>Traffic Status .....</b>	<b>247</b>
18.1 Overview .....	247
18.1.1 What You Can Do in this Chapter .....	247
18.2 The WAN Status Screen .....	247
18.3 The LAN Status Screen .....	248
18.4 The NAT Status Screen .....	249
18.5 The 3G Backup Status Screen .....	250
18.6 The VoIP Status Screen .....	251
<b>Chapter 19</b>	
<b>User Account .....</b>	<b>253</b>
19.1 Overview .....	253
19.2 The User Account Screen .....	253
<b>Chapter 20</b>	
<b>Remote MGMT.....</b>	<b>255</b>
20.1 Overview .....	255
20.1.1 What You Need to Know .....	255
20.2 The Remote MGMT Screen .....	256

<b>Chapter 21</b>	
<b>System .....</b>	<b>257</b>
21.1 Overview .....	257
21.1.1 What You Need to Know .....	257
21.2 The System Screen .....	257
<b>Chapter 22</b>	
<b>Time Setting .....</b>	<b>259</b>
22.1 Overview .....	259
22.2 The Time Setting Screen .....	259
<b>Chapter 23</b>	
<b>Log Setting .....</b>	<b>261</b>
23.1 Overview .....	261
23.2 The Log Setting Screen .....	261
<b>Chapter 24</b>	
<b>Firmware Upgrade .....</b>	<b>263</b>
24.1 Overview .....	263
24.2 The Firmware Upgrade Screen .....	263
<b>Chapter 25</b>	
<b>Backup/Restore .....</b>	<b>265</b>
25.1 Overview .....	265
25.2 The Backup/Restore Screen .....	265
25.3 The Reboot Screen .....	267
<b>Chapter 26</b>	
<b>Diagnostic .....</b>	<b>269</b>
26.1 Overview .....	269
26.2 The Ping/TraceRoute Screen .....	269
26.3 The DSL Line Screen .....	270
<b>Chapter 27</b>	
<b>Troubleshooting.....</b>	<b>273</b>
27.1 Overview .....	273
27.2 Power, Hardware Connections, and LEDs .....	273
27.3 Device Access and Login .....	274
27.4 Internet Access .....	276
27.5 Wireless Internet Access .....	278
27.6 Phone Calls and VoIP .....	279
27.7 USB Device Connection .....	279
27.8 UPnP .....	279

<b>Chapter 28</b>	
<b>Product Specifications .....</b>	<b>281</b>
Appendix A IP Addresses and Subnetting .....	289
Appendix B Setting Up Your Computer's IP Address .....	299
Appendix C Pop-up Windows, JavaScript and Java Permissions .....	329
Appendix D Wireless LANs.....	339
Appendix E Common Services .....	359
Appendix F IPv6 .....	363
Appendix G Open Software Announcements .....	375
Appendix H Legal Information .....	411
<b>Index .....</b>	<b>415</b>

---

# **PART I**

## **User's Guide**

---





# Introduction

## 1.1 Overview

The Device is a VDSL, ADSL and Ethernet WAN router, which also includes Voice over IP (VoIP) communication capabilities to allow you to use a traditional analog telephone to make Internet calls. By integrating all of these features, you are provided with ease of installation and high-speed, shared Internet access. The Device is also a complete security solution with a robust firewall based on Stateful Packet Inspection (SPI) technology and Denial of Service (DoS).

Please refer to the following description of the product name format.

- “H” denotes an integrated 4-port hub (switch).
- “N” denotes wireless functionality, including 802.11n mode. There is an embedded mini-PCI module for IEEE 802.11 b/g/n wireless LAN connectivity.
- “U” denotes a USB port used to set up a 3G WAN connection via a 3G wireless card or share files via a USB memory stick or a USB hard drive. The Device can function as a print server with an USB printer connected.
- “L” denotes the PSTN (Public Switched Telephone Network) line feature. The PSTN line lets you have VoIP phone service and PSTN phone service at the same time. All PSTN line features documented in this user’s guide refer to the “L” models only.

**When the Device does not have power, only the phone connected to the PHONE port 1 can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.**

- Models ending in “1”, for example P-2812HNU(L)-F1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3”, for example P-2812HNU(L)-F3, denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

See the chapter on product specifications for a full list of features.

## 1.2 Applications for the Device

Here are some example uses for which the Device is well suited.

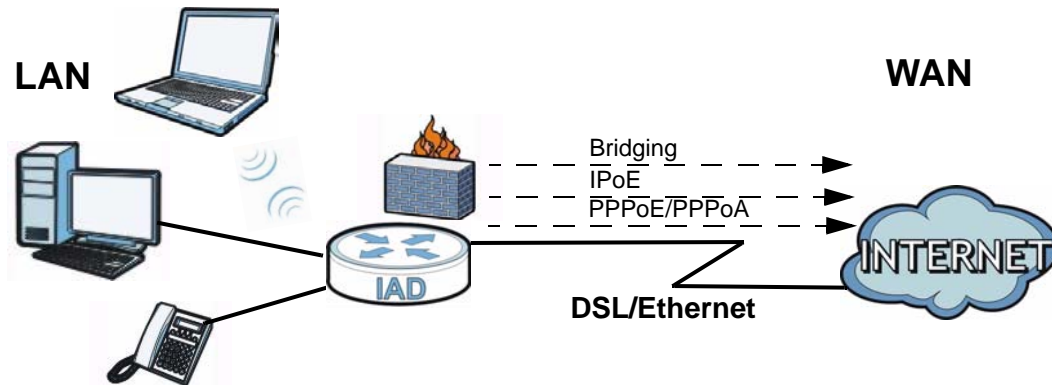
### 1.2.1 Internet Access

Your Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. If you prefer not to use a DSL line and you have another broadband modem or router (such as ADSL) available, you can set the WAN mode to **EtherWAN** in

the **Broadband** screen (see [Chapter 5 on page 91](#) for more information) and connect the **WAN** port to the broadband modem or router. This way, you can access the Internet via an Ethernet connection and still use the QoS, Firewall and VoIP functions on the Device.

Computers can connect to the Device's LAN ports (or wirelessly).

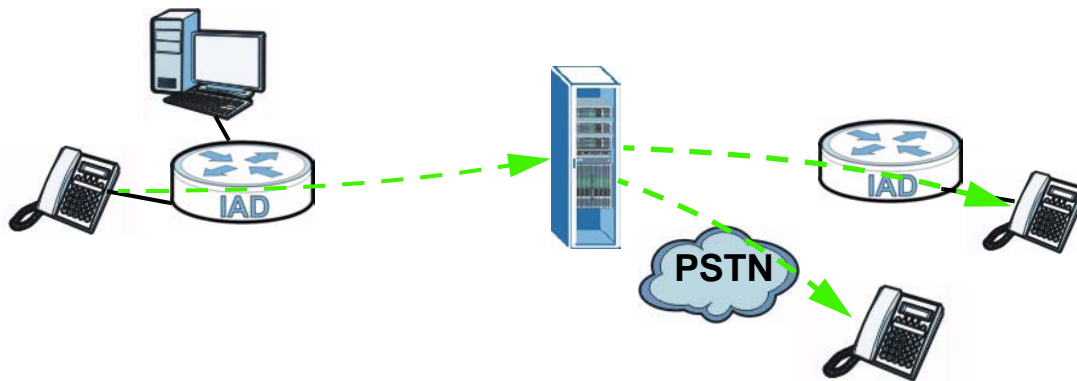
**Figure 1** Device's Internet Access Application



## 1.2.2 VoIP Features

You can register 1 SIP (Session Initiation Protocol) profile (2 accounts for that profile) and use the Device to make and receive VoIP telephone calls:

**Figure 2** Device's VoIP Application



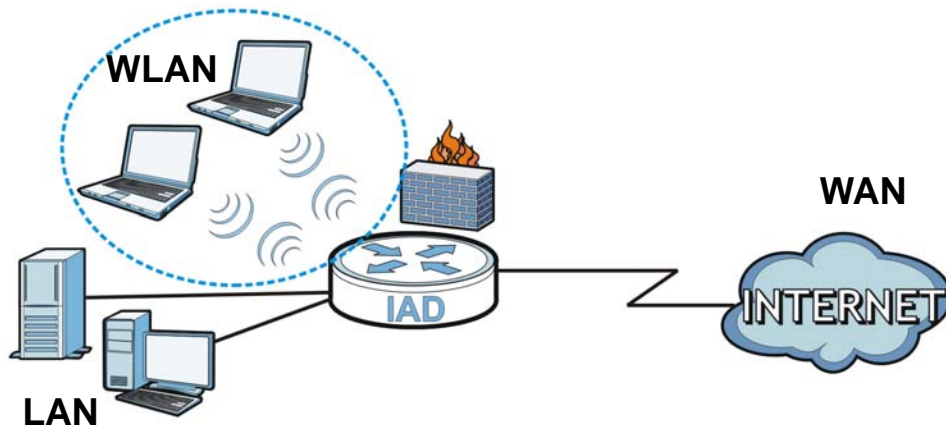
The Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

## 1.2.3 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the Device. Once Wireless is enabled, IEEE 802.11b/g/n compliant clients can wirelessly connect to the Device to access network resources.

You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

**Figure 3** Wireless Connection Application



## 1.3 The WLAN Button

You can use the **WLAN ON/OFF** button on top of the device to turn the wireless LAN on or off. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

### Turn the Wireless LAN On or Off

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Press the **WLAN ON/OFF** button for one second and release it. The **WLAN/WPS** LED should change from on to off or vice versa.

### Activate WPS

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Press the **WLAN ON/OFF** button for more than five seconds and release it. Press the WPS button on another WPS-enabled device within range of the Device. The **WLAN/WPS** LED should flash while the Device sets up a WPS connection with the wireless device.

Note: You must activate WPS in the Device and in another wireless device within two minutes of each other. See [Chapter 6 on page 142](#) for more information.

# 1.4 Ways to Manage the Device

Use any of the following methods to manage the Device.

- Web Configurator. This is recommended for everyday management of the Device using a (supported) web browser.
- FTP for firmware upgrades and configuration backup/restore.

# 1.5 Good Habits for Managing the Device

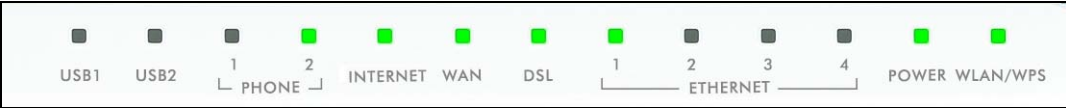
Do the following things regularly to make the Device more secure and to manage the Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password to access the Web Configurator, you will have to reset the Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Device. You could simply restore your last configuration. Keep in mind that backing up a configuration file will not back up passwords used to set up PPPoE and VoIP. Write down any information your ISP provides you.

# 1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

**Figure 4** LEDs on the Top of the Device



None of the LEDs are on if the Device is not receiving power.

**Table 1** LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
USB1-2	Green	On	The Device recognizes a USB connection but there is no traffic.
		Blinking	The Device is sending/receiving data to /from the USB device connected to it.
	Off		The Device does not detect a USB connection.

**Table 1** LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
PHONE1-2	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
	Off		The phone port does not have a SIP account registered.
INTERNET	Green	On	The Device has an IP connection but no traffic.  Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used).
		Blinking	The Device is sending or receiving IP traffic.
		Off	The Device does not have an IP connection.
	Red	On	The Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
WAN	Green	On	This light applies when the Device is in Ethernet WAN mode. The Device has an Ethernet connection with a device on the WAN.
		Blinking	The Device is sending or receiving data to/from the Ethernet WAN.
		Off	The Device does not have an Ethernet connection with the WAN.
DSL	Green	On	The VDSL line is up.
		Blinking	The Device is initializing the VDSL line.
	Orange	On	The ADSL line is up.
		Blinking	The Device is initializing the ADSL line.
		Off	The DSL line is down.
ETHERNET1-4	Green (Giga Ethernet)	On	The Device has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Device is sending or receiving data to/from the LAN at 1000 Mbps.
	Orange (Fast Ethernet)	On	The Device has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Device is sending or receiving data to/from the LAN at 10/100 Mbps.
	Off		The Device does not have an Ethernet connection with the LAN.
POWER	Green	On	The Device is receiving power and ready for use.
		Blinking	The Device is self-testing.
	Red	On	The Device detected an error while self-testing, or there is a device malfunction.
	Off		The Device is not receiving power.

**Table 1** LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
WLAN/WPS	Green	On	The wireless network is activated and is operating in IEEE 802.11 "b", "g" or "n" mode.
		Blinking	The Device is communicating with other wireless clients.
	Orange	On	The WPS is configured.
		Blinking	The Device is setting up a WPS connection.
	Off		The wireless network is not activated.

Refer to the Quick Start Guide for information on hardware connections.

## 1.7 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the passwords will be reset to the defaults.

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button for 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

# Introducing the Web Configurator

## 2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See [Appendix C on page 329](#) if you need to make sure these functions are allowed in Internet Explorer.

### 2.1.1 Accessing the Web Configurator

- 1 Make sure your Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 A password screen displays. Type "admin" as the default Username and "1234" as the default password to access the device's Web Configurator. Click **Login**. If you have changed the password, enter your password and click **Login**.

**Figure 5** Password Screen



Note: For security reasons, the Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

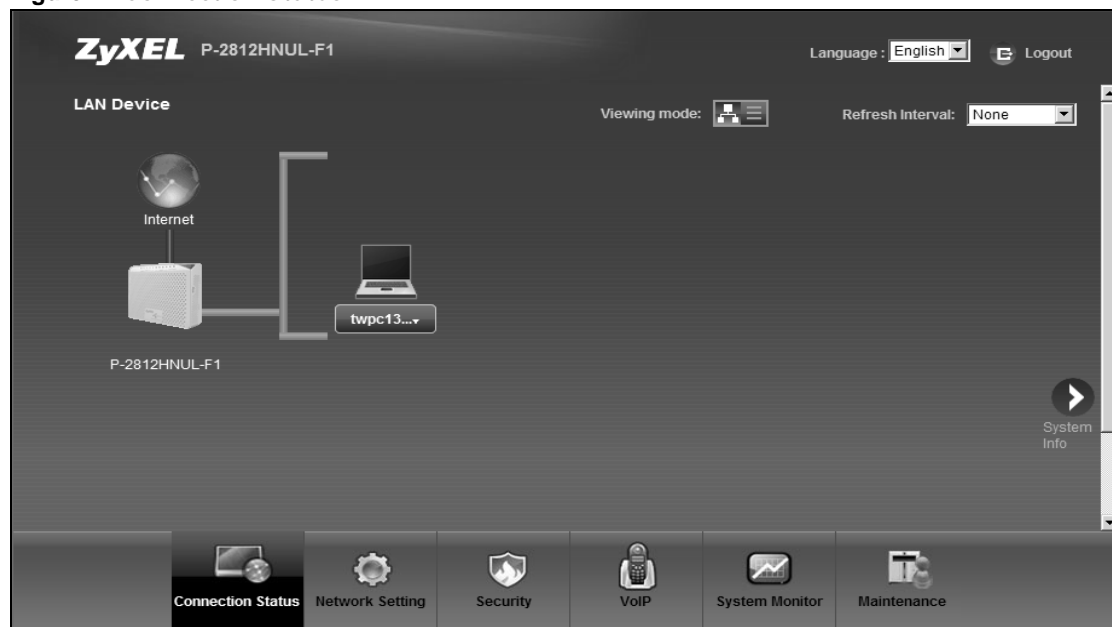
- 5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the main menu if you do not want to change the password now.

**Figure 6** Change Password Screen

The screenshot shows the ZyXEL Change Password screen. On the left is a large padlock icon. The text reads: "Change Password", "It is highly recommended to setup a new password instead of using the default one for security concern.", "New Password:", "Verify New Password:", and two input fields. At the bottom right are "Skip" and "Apply" buttons.

- 6 The **Connection Status** screen appears.

**Figure 7** Connection Status



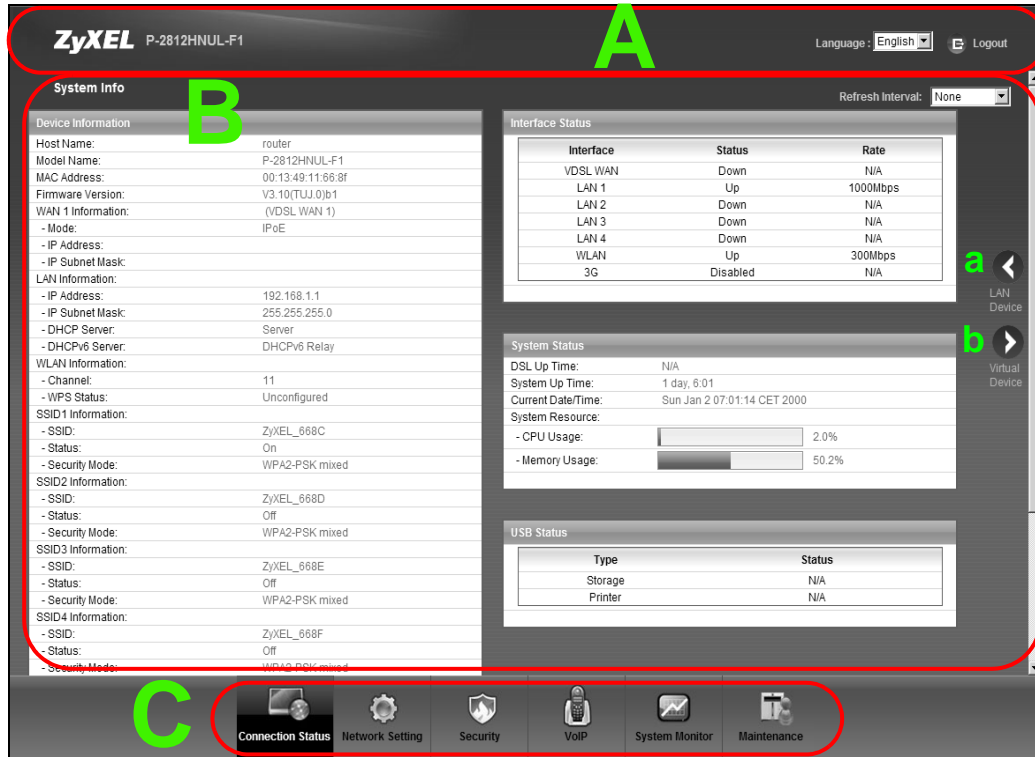
- 7 Click **System Info** to display the **System Info** screen, where you can view the Device's interface and system information.



## 2.2 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen.

**Figure 8** Web Configurator Layout



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - navigation panel

### 2.2.1 Title Bar

The title bar shows the following icon in the upper right corner.



Click this icon to log out of the web configurator.

### 2.2.2 Main Window

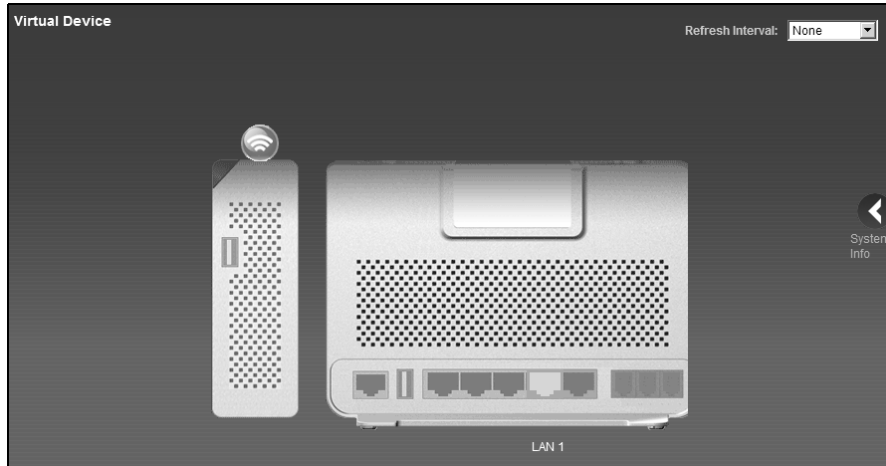
The main window displays information and configuration fields. It is discussed in the rest of this document.

After you click **System Info** on the **Connection Status** screen, the **System Info** screen is displayed. See [Chapter 4 on page 83](#) for more information about the **System Info** screen.

If you click **LAN Device** on the **System Info** screen (a in Figure 8 on page 29), the **Connection Status** screen appears. See Chapter 4 on page 81 for more information about the **Connection Status** screen.

If you click **Virtual Device** on the **System Info** screen (b in Figure 8 on page 29), a visual graphic appears, showing the connection status of the Device's ports. The connected ports are in color and disconnected ports are gray.

**Figure 9** Virtual Device



## 2.2.3 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Device features. The following table describes each menu item.

**Table 2** Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and modify your WAN interface. You can also configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	3G Backup	Use this screen to configure the 3G WAN connection.
Wireless	General	Use this screen to turn the wireless connection on or off, specify the SSID(s) and configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the Device.
	WPS	Use this screen to use WPS (Wi-Fi Protected Setup) to establish a wireless connection.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Scheduling	Use this screen to configure when the Device enables or disables the wireless LAN.

**Table 2** Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to enable the UPnP function.
	File Sharing	Use this screen to enable file sharing via the Device.
	Media Server	Use this screen to enable or disable the sharing of media files.
	Printer Server	Use this screen to enable or disable sharing of a USB printer via your Device.
Static Route	Static Route	Use this screen to view and set up static routes on the Device.
DNS Route	DNS Route	Use this screen to view and configure DNS routes.
QoS	General	Use this screen to enable QoS and decide allowable bandwidth using QoS.
	Queue Setup	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
	Monitor	Use this screen to view each queue's statistics.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Sessions	Use this screen to limit the number of NAT sessions a single client can establish.
Dynamic DNS	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	Use this screen to set the default action to take on outgoing network traffic.
MAC Filter	MAC Filter	Use this screen to allow specific devices to access the Device.
Parental Control	Parental Control	Use this screen to define time periods and days during which the Device performs parental control and/or block web sites with the specific URL.
Certificates	Local Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the Device's CA-signed certificates.
	Trusted CA	Use this screen to save CA certificates to the Device.
VoIP		
SIP	SIP Service Provider	Use this screen to configure your Device's Voice over IP settings.
	SIP Account	Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the Device.
	Common	Use this screen to configure RFC3262 support on the Device.

**Table 2** Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Phone	Phone Device	Use this screen to set which phone ports use which SIP accounts.
	Region	Use this screen to select your location.
Call Rule	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
FXO	FXO Device	Use this screen to set up the PSTN line you use to make regular phone calls.
System Monitor		
Log	Phone Log	Use this screen to view the Device's phone logs.
	VoIP Call History	Use this screen to view the Device's VoIP call history.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Device.
	NAT	Use this screen to view the status of NAT sessions on the Device.
	3G Backup	Use this screen to view the status of 3G Backup on the Device.
VoIP Status	VoIP Status	Use this screen to view the SIP, phone, and call status of the Device.
Maintenance		
Users Account	Users Account	Use this screen to configure the passwords your user accounts.
Remote MGMT	Remote MGMT	Use this screen to enable specific traffic directions for network services.
System	System	Use this screen to configure the Device's name, domain name, management inactivity time-out.
Time	Time Setting	Use this screen to change your Device's time and date.
Log Setting	Log Setting	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Device without turning the power off.
Diagnostic	Ping/TraceRoute	Use this screen to test the connections to other devices.
	DSL Line	Use this screen to identify problems with the DSL connection.

## 3.1 Overview

This chapter contains the following tutorials:

- [Setting Up Your DSL Connection](#)
- [How to Set up a Wireless Network](#)
- [Setting Up NAT Port Forwarding](#)
- [How to Make a VoIP Call](#)
- [Using the File Sharing Feature](#)
- [Using the Media Server Feature](#)
- [Using the Print Server Feature](#)
- [Configuring the MAC Address Filter](#)
- [Configuring Static Route for Routing to Another Network](#)
- [Configuring QoS Queue and Class Setup](#)
- [Access the Device Using DDNS](#)

## 3.2 Setting Up Your DSL Connection

This tutorial shows you how to set up your Internet connection using the web configurator.

If you connect to the Internet through a DSL connection, use the information from your Internet Service Provider (ISP) to configure the Device. Do the following steps:

- 1 Connect the Device properly. Refer to the Quick Start Guide for details on the Device's hardware connection.
- 2 Connect one end of a DSL cable to the DSL port of your Device. The other end should be connected to the DSL port in your house or a DSL router/modem provided by your ISP.
- 3 Connect one end of Ethernet cable to an Ethernet port on the Device and the other end to a computer that you will use to access the web configurator.
- 4 Connect the Device to a power source, turn it on and wait for the **POWER** LED to become a steady green. Turn on the modem provided by your ISP as well as the computer.

### Account Configuration

- 1 Click **Network Setting** > **Broadband** to open the **Broadband** screen.

- 2 Select **ADSL** as your WAN mode type and click **Switch WAN Interface**.

**Switch WAN Mode**

Type : ADSL ▼ Switch WAN Interface

Add new WAN Interface

**Internet Setup**

#	Name	Type	Mode	Encap...	IPv6	VPI	VCI	Vlan80...	VlanM...	ATM Q...	IGMP ...	NAT	Defaul...	Modify
1	EtherW...	EtherW...	Routing	IPoE	Disable	N/A	N/A	N/A	N/A	N/A	Enabled	Enabled	Yes	
2	AdslW...	ADSL	Routing	IPoE	Disable	8	35	N/A	N/A	UBR	Enabled	Enabled	Yes	
3	VdslW...	VDSL	Routing	IPoE	Disable	N/A	N/A	N/A	N/A	N/A	Enabled	Enabled	Yes	

- 3 Confirm your selection and wait for the Device to reboot.
- 4 Log into the Device again and go to the **Network Setting > Broadband** screen. Click **Add new WAN Interface**.
- 5 For this example, the interface type is ADSL and the connection has the following information.

General	
Name	MyDSLConnection
Type	ADSL
Mode	Routing
WAN Service Type	PPPoE
ATM PVC Configuration	
VPI/VCI	36/48
Encapsulation Mode	LLC/SNAP-Bridging
Service Category	UBR without PCR
PPP Information	
PPP User Name	1234@DSL-Ex.com
PPP Password	ABCDEF!
PPPoE Service Name	My DSL
Authentication Method	Auto
Static IP Address	192.168.1.32
Others	PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enable DNS Server: Static DNS IP Address (Primary: 192.168.1.254 Secondary: 192.168.1.253)

Enter or select these values and click **Apply**.

**General**

Name : MyDSLConnection  
Type : ADSL  
Mode : Routing  
WANSERVICEType : PPP over Ethernet(PPPoE)  
PPPoE Passthrough : ☐  
IPv6/IPv4 DualStack : Disable

**ATM PVC Configuration**

VPI[0-255] : 36  
VCI[32-65535] : 48  
DSL Link Type : EoA  
Encapsulation Mode : LLC/SNAP-BRIDGING  
Service Category : UBR Without PCR

**PPP Information**

PPPOEUserName : 234@DSL-Ex.com  
PPPOEPassword : .....  
PPPOESERVICEName : My DSL  
Authentication Method : Auto  
Use Static IP Address : ☒  
IP Address : 192.168.1.32

**Routing Feature**

NAT Enable : ☒  
IGMP Proxy Enable : ☒  
Apply as Default Gateway : ☒

**DNS Server**

☐ Obtain DNS info Automatically  
☒ Use the following Static DNS IP Address  
Primary DNS Server : 192.168.1.254  
Secondary DNS Server : 192.168.1.253

Apply Back

This completes your DSL WAN connection setting.

- 6 You should see a summary of your new DSL connection setup in the **Broadband** screen as follows.

Switch WAN Mode  
Type : ADSL Switch WAN Interface

Add new WAN Interface

Internet Setup

#	Name	Type	Mode	Encapsula...	IPv6	VPI	VCI	Vlan8021p	VlanMuxid	ATM QoS	IGMP Proxy	NAT	Default Gat...	Modify
1	EtherWAN1	EtherWAN	Routing	IPoE	Disable	N/A	N/A	N/A	N/A	N/A	Enabled	Enabled	Yes	
2	AdsIWAN1	ADSL	Routing	IPoE	Disable	8	35	N/A	N/A	UBR	Disabled	Enabled	No	
3	MyDSLCon...	ADSL	Routing	PPPoE	Disable	36	48	N/A	N/A	UBR	Enabled	Enabled	Yes	
4	VdsIWAN1	VDSL	Routing	IPoE	Disable	N/A	N/A	N/A	N/A	N/A	Enabled	Enabled	Yes	

Try to connect to a website, such as “www. zyxel.com” to see if you have correctly set up your Internet connection. Be sure to contact your service provider for any information you need to configure the WAN screens.

## 3.3 How to Set up a Wireless Network

This section gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through the Device wirelessly.

### 3.3.1 Example Parameters

<b>SSID</b>	SSID_Example3
<b>802.11 mode</b>	802.11b/g
<b>Channel</b>	auto
<b>Security</b>	WPA-PSK (Pre-Shared Key: 12MyWPAPSKpresharedkey34)

An access point (AP) or wireless router is referred to as the “AP” and a computer with a wireless network card or USB adapter is referred to as the “wireless client” here.

We use the M-302 utility screens as the wireless client example. The screens may vary for different models.

### 3.3.2 Configuring the AP

Follow the steps below to configure the wireless settings on your AP.



- 1 Open the **Network Setting > Wireless > General** screen in the AP's web configurator.

**Wireless Network Setup**

Wireless : ☒ Enable Wireless LAN

**Wireless Network Settings**

Wireless Network Name(SSID):

☐ Hide SSID

BSSID : 02:13:49:11:66:8c

Mode Select :

Channel Selection :

Operating Channel : 6

**Security Level**

No Security Basic **More Secure (Recommended)**

Security Mode :

Enter 8-63 characters (a-z, A-Z, and 0-9) or 64 hexadecimal digits (a-f, A-F, and 0-9).

Pre-Shared Key :

- 2 Make sure **Enable Wireless LAN** is selected.
- 3 Enter "SSID\_Example3" as the SSID and select **Auto** in the **Channel Selection** field to have the device search for an available channel.
- 4 Select **802.11b/g** in the **Mode Select** field.
- 5 Select **More Secure** as your security level and set security mode to **WPA-PSK** and enter "12MyWPAPSKpresharedkey34" in the **Pre-Shared Key** field. Click **Apply**.
- 6 Click **Connection Status > System Info**. Verify your wireless and wireless security settings under **Device Information** and check if the **WLAN** connection is up under **Interface Status**.

**System Info**

Refresh Interval:

**Device Information**

Host Name: router

Model Name: P-2812HNUL-F1

MAC Address: 00:13:49:11:66:8f

Firmware Version: V3.10(TUJ.0)b4

WAN 1 Information: (ADSL WAN 1)

- Mode: EoA

- IP Address:

- IP Subnet Mask:

WAN 2 Information: (ADSL WAN 2)

- Mode: PPPoE

- IP Address:

LAN Information:

- IP Address: 192.168.1.1

- IP Subnet Mask: 255.255.255.0

- DHCP Server: Server

- DHCPv6 Server: DHCPv6 Relay

**WLAN Information:**

- Channel: 6

- WPS Status: Configured

**SSID 1 Information:**

- SSID: SSID\_Example3

- Status: On

- Security Mode: WPA-PSK

**SSID 2 Information:**

- SSID: ZyXEL\_668D

- Status: Off

- Security Mode: WPA2-PSK mixed

**Interface Status**

Interface	Status	Rate
ADSL WAN	Down	N/A
LAN 1	Up	1000Mbps
LAN 2	Down	N/A
LAN 3	Down	N/A
LAN 4	Down	N/A
<b>WLAN</b>	<b>Up</b>	<b>54Mbps</b>
3G	Disabled	N/A

**System Status**

DSL Up Time: N/A

System Up Time: 22 min

Current Date/Time: Sat Jan 1 01:22:00 CET 2000

System Resource:

- CPU Usage:

- Memory Usage:

**USB Status**

Type	Status
Storage	N/A

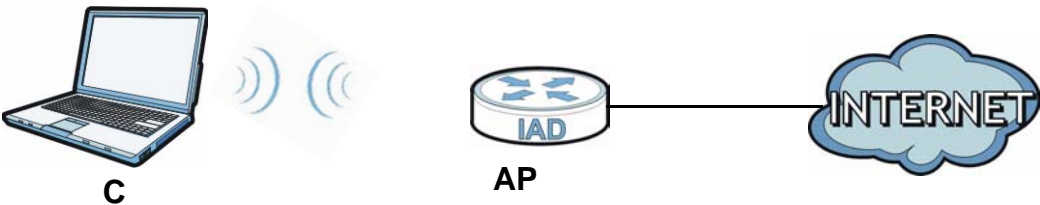
This finishes the configuration of the AP.

### 3.3.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

#### 3.3.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



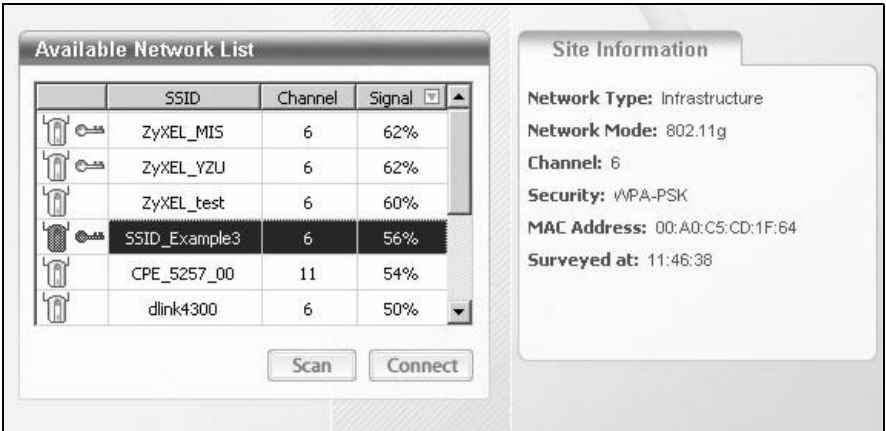
There are three ways to connect the client to an access point.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is "SSID\_Example3" and the pre-shared key is "12MyWPAPSKpresharedkey34".

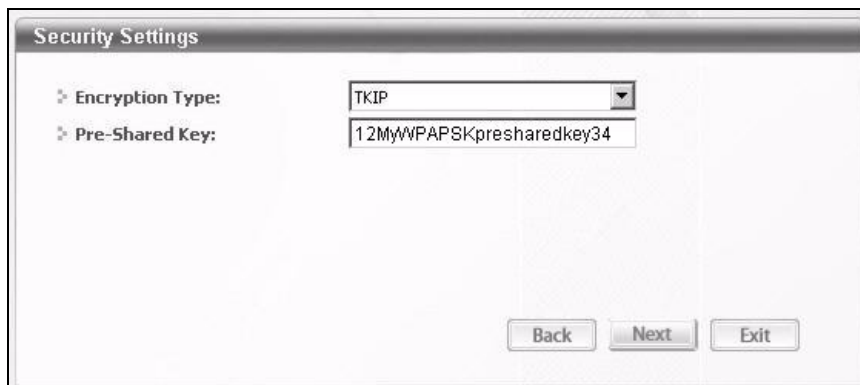
After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

- 1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.



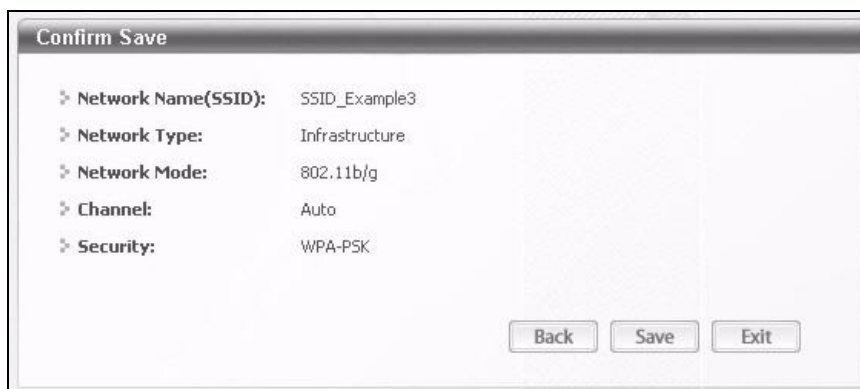
- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.
- 3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.



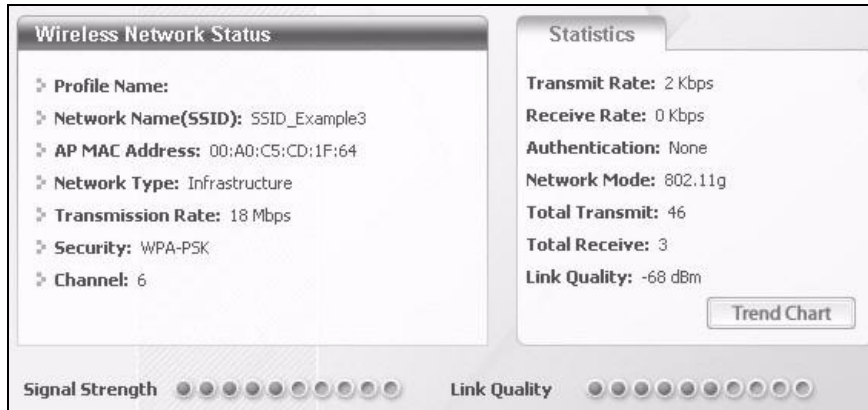
The **Security Settings** dialog box contains two fields: **Encryption Type:** with a dropdown menu showing **TKIP**, and **Pre-Shared Key:** with a text box containing **12MyWPAPSKpresharedkey34**. At the bottom right are three buttons: **Back**, **Next**, and **Exit**.

- 4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.



The **Confirm Save** dialog box displays a summary of network settings: **Network Name(SSID):** SSID\_Example3, **Network Type:** Infrastructure, **Network Mode:** 802.11b/g, **Channel:** Auto, and **Security:** WPA-PSK. At the bottom right are three buttons: **Back**, **Save**, and **Exit**.

- The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.



- Open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

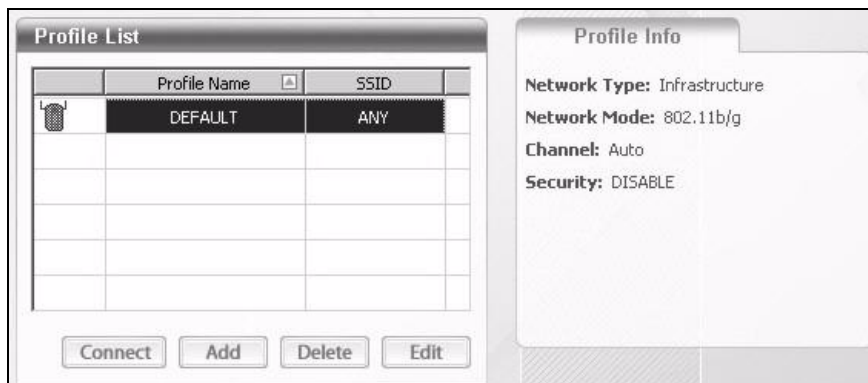
If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

### 3.3.3.2 Creating and Using a Profile

A profile lets you easily connect to the same wireless network again later. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an AP configured for WPA-PSK security. In this example, the SSID is "SSID\_Example3", the profile name is "PN\_Example3" and the pre-shared key is "". You have chosen the profile name "PN\_Example3".

- Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.



- The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, and displays them in the **Scan Info** box. Click **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

	SSID
	CPE_5257_00
	CPE_5548_AP
	SSID_Example3
	zld_zyxel
	ZyXEL

Buttons: Scan, Select

- Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.
- Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

Encryption Type: WPA-PSK

Buttons: Back, Next, Exit

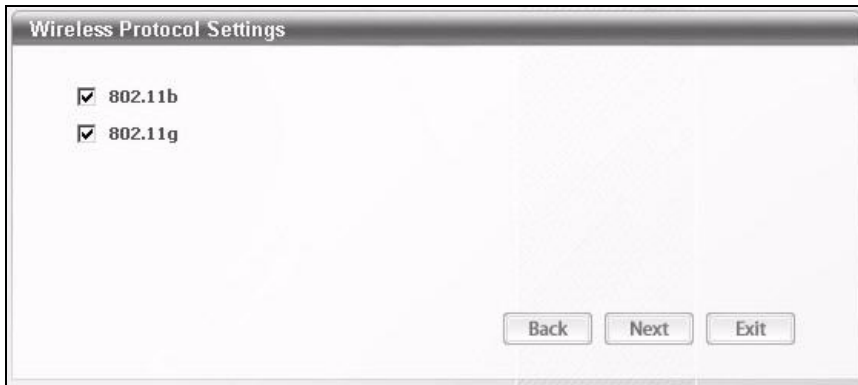
- This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

Encryption Type: TKIP

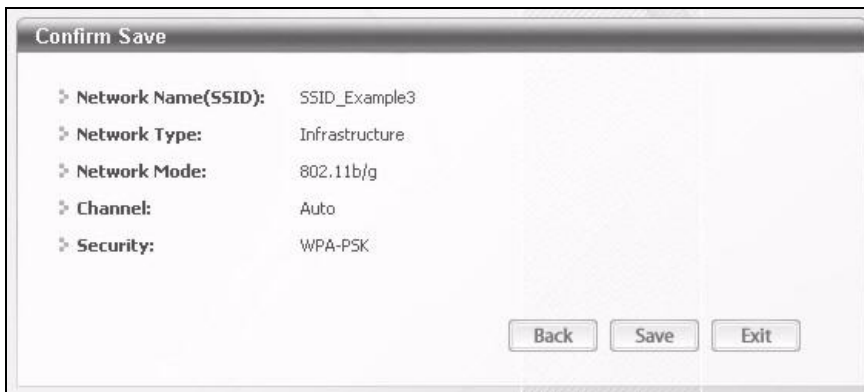
Pre-Shared Key: 12MyWPAPSKpresharedkey34

Buttons: Back, Next, Exit

- 6 In the next screen, leave both boxes selected.



- 7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.



- 8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

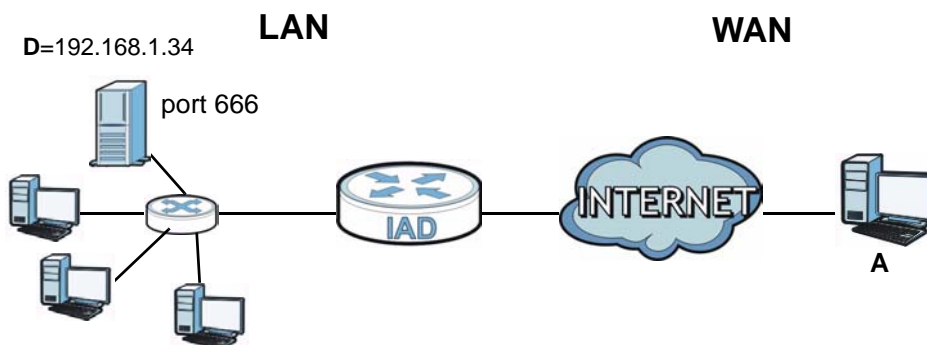


- 9 When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.
- 10 Open your Internet browser, enter <http://www.zyxel.com> or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

- 11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

## 3.4 Setting Up NAT Port Forwarding

In this tutorial, you manage the Doom server on a computer behind the Device. In order for players on the Internet (like **A** in the figure below) to communicate with the Doom server, you need to configure the port settings and IP address on the Device. Traffic should be forwarded to the port 666 of the Doom server computer which has an IP address of 192.168.1.34.



You may set up the port settings by configuring the port settings for the Doom server computer (see [Chapter 10 on page 190](#) for more information).

- 1 Click **Network Setting > NAT > Port Forwarding**. Click **Add new rule**.

- 2 Enter the following values:

Service Name	Select <b>User Defined</b> .
WAN Interface	Select the WAN interface through which the Doom service is forwarded. This is the default interface for this example, which is <b>MyDSLConnection</b> .
Start/End Ports	<b>666</b>
Translation Start/End Ports	<b>666</b>
Server IP Address	Enter the IP address of the Doom server. This is <b>192.168.1.34</b> for this example.
Protocol	Select <b>TCP/UDP</b> . This should be the protocol supported by the Doom server.

- 3 Click **Apply**.
- 4 The port forwarding settings you configured should appear in the table. Make sure the bulb in **Status** is the color yellow, meaning it is activated. Click **Apply** to have the Device start forwarding port 666 traffic to the computer with IP address 192.168.1.34.

Add new rule										
#	Status	Service Name	WAN Interface	Start Port	End Port	Translation Start Port	Translation End Port	Server IP Address	Protocol	Modify
1		User Defined	MyDSLConn	666	666	666	666	192.168.1.34	TCP/UDP	

Players on the Internet then can have access to your Doom server.

## 3.5 How to Make a VoIP Call

You can register a SIP account with the SIP server and make voice calls over the Internet to another VoIP device.



The following parameters are used in this example:

<b>SIP Service Provider Name</b>	ServiceProvider1
<b>SIP Server Address</b>	sip.example.com
<b>REGISTER Server Address</b>	registersip.example.com
<b>SIP Service Domain</b>	sip.example.com
<b>SIP Account Number</b>	12345678
<b>Username</b>	ChangeMe
<b>Password</b>	ThisIsMySIP

### 3.5.1 VoIP Calls With a Registered SIP Account

To use a registered SIP account, you should configure the SIP service provider and applied for a SIP account.

#### 3.5.1.1 SIP Service Provider Configuration

Follow the steps below to configure your SIP service provider.

- 1 Make sure your Device is connected to the Internet.
- 2 Open the web configurator.
- 3 Click **VoIP > SIP** to open the **SIP Service Provider** screen. Select **ChangeMe** from the **Service Provider Selection** drop-down list box.
- 4 Select the **Enable** check box of **SIP Service Provider** and enter **ServiceProvider1** as the **SIP Service Provider Name**. Enter the **SIP Server Address**, **REGISTER Server Address**, and **SIP Service Domain** provided by your ISP accordingly. Click **Apply**.

**SIP Service Provider Selection**

Service Provider Selection : ChangeMe Delete

**General**

SIP Service Provider : ☒ Enable SIP Service Provider

SIP Service Provider Name :

SIP Local Port :  (1025-65535)

SIP Server Address :

SIP Server Port :  (1025-65535)

REGISTER Server Address :

REGISTER Server Port :  (1025-65535)

SIP Service Domain :

[more...](#)

Apply Cancel

- 5 Go to the **SIP Account** screen, click the **Edit** icon of **SIP 1**.

Add new SIP account					
#	Active	SIP Account	SIP Service Provider	Account No.	Modify
1		SIP 1	ServiceProvider1	ChangeMe	
2		SIP 2	ServiceProvider1	ChangeMe	

- 6 Select the **Active SIP Account** check box, then enter the **SIP Account Number**, **Username**, and **Password**. Leave other settings as default.
- 7 Click **Apply** to save your settings.

**SIP Service Provider Selection**

Service Provider Selection : ServiceProvider1

**SIP Account Selection**

SIP Account Selection : SIP 1

**General**

SIP Account : ☒ Active SIP Account

SIP Account Number :

**Authentication**

Username :

Password :

### 3.5.1.2 SIP Account Registration



Follow the steps below to register and activate your SIP account.

- 1 Click **Connection Status > System Info** to check if your SIP account has been registered successfully. If the status is **Not Registered**, check your Internet connection and click **Register** to register your SIP account.

Registration Status			
Account	Action	Account Status	URI
SIP 1		Not Registered	12345678@sip.example.com
SIP 2		In-Active	ChangeMe@sip.example.com

### 3.5.1.3 Analog Phone Configuration

- 1 Click **VoIP > Phone** to open the **Phone Device** screen. Click the **Edit** icon next to **Analog Phone 1** to configure the first phone port.

Analog Phone			
#	Phone ID	Outgoing SIP Number	Modify
1	Analog Phone 1	12345678	
2	Analog Phone 2	ChangeMe	

- 2 Select **SIP 1** from the **SIP Account** in the **SIP Account to Make Outgoing Call** section to have the phone (connected to the first phone port) use the registered SIP 1 account to make outgoing calls.
- 3 Select the **SIP 1** check box in the **SIP Account(s) to Receive Incoming Call** section to have the phone (connected to the first phone port) receive phone calls for the SIP 3 account.
- 4 Click **Apply** to save your changes.

SIP Account to Make Outgoing Call			
SIP Account	SIP Number	SIP Account	SIP Number
<input checked="" type="radio"/> SIP 1	12345678	<input type="radio"/> SIP 2	ChangeMe

SIP Account(s) to Receive Incoming Call			
SIP Account	SIP Number	SIP Account	SIP Number
<input checked="" type="checkbox"/> SIP 1	12345678	<input type="checkbox"/> SIP 2	ChangeMe

**FXO Interface to Receive Incoming Call**

☒ Enable

### 3.5.1.4 Making a VoIP Call

- 1 Make sure you connect a telephone to the first phone port on the Device.
- 2 Make sure the Device is on and connected to the Internet.
- 3 Pick up the phone receiver.
- 4 Dial the VoIP phone number you want to call.

## 3.6 Using the File Sharing Feature

In this section you can:

- Set up file sharing of your USB device from the Device

- Access the shared files of your USB device from a computer

### 3.6.1 Set Up File Sharing

To set up file sharing you need to connect your USB device, enable file sharing and set up your share(s).

#### 3.6.1.1 Activate File Sharing

- 1 Connect your USB device to one of the USB ports at the back panel of the Device.
- 2 Click **Network Setting > Home Networking > File Sharing**. Select **Enable** and click **Apply** to activate the file sharing function. The Device automatically adds your USB device to the **Share Directory List**.

**Server Configuration**

File Sharing Services(SMB): ☒ Enable ☐ Disable

**Share Directory List**

[Add new share](#)

#	Status	Share Name	Share Path	Share Description	Modify
1	<input checked="" type="checkbox"/>	USB_Storage	GENERIC_USB_Mass_Storage_100_1	USB_Storage	

[Apply](#) [Cancel](#)

#### 3.6.1.2 Set up File Sharing on Your Device

You also need to set up file sharing on your Device in order to share files.

- 1 Click **Add new share** in the **File Sharing** screen to configure a new share. Select your USB device from the **Volume** drop-down list box.
- 2 Click **Browse** to browse through all the files on your USB device. Select the folder that you want to add as a share. In this example, select **Bob's\_Share**. Click **Apply**.

• **GENERIC\_USB\_Mass\_Storage\_100\_1**

Select	Type	Name	Date
<input type="radio"/>		.	N/A
<input checked="" type="radio"/>		Bob's_Share	2010-08-25 09:45:26
<input type="radio"/>		Mac	2010-08-17 09:38:36
<input type="radio"/>		zywall-1050_dir	2003-01-01 06:08:00
<input type="radio"/>		Win 7	2010-04-27 14:51:36
<input type="radio"/>		NWD-2205_(PowerPC)MacOS10.4_Driver_1003_UI_1.7.9	2010-08-17 15:15:16
<input type="radio"/>		RECYCLER	2010-08-22

[Apply](#) [Back](#)

- 3 You can add a description for the share or leave it blank. The **Add Share Directory** screen should look like the following. Click **Apply** to finish.

- 4 This sets up the file sharing server. You can see the USB storage device listed in the table below.

Share Directory List

Add new share

#	Status	Share Name	Share Path	Share Description	Modify
1		GENERIC_USB_Mass_Storage...	GENERIC_USB_Mass_Storage_100_1	GENERIC_USB_Mass_Storage_100_1	
2		USB_Storage	GENERIC_USB_Mass_Storage_100_1	USB_Storage	

Apply Cancel

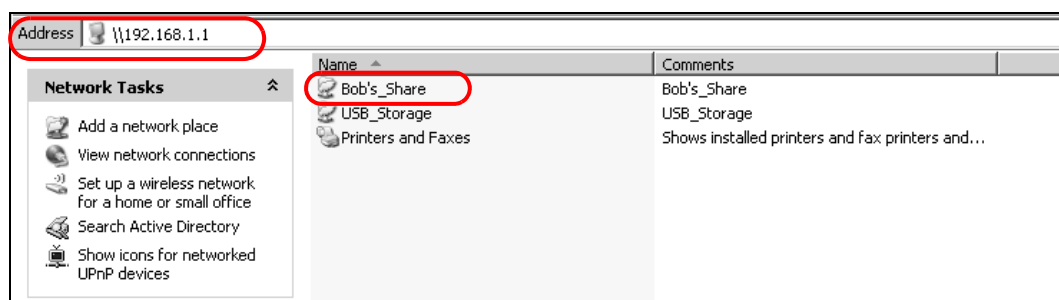
## 3.6.2 Access Your Shared Files From a Computer

You can use Windows Explorer to access the file storage devices connected to the Device.

Note: The examples in this User's Guide show you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Open Windows Explorer to access Bob's Share using Windows Explorer browser.

In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the Device (the default IP address of the Device is 192.168.1.1) and press [ENTER]. The share folder **Bob's\_Share** is available.



Once you access **Bob's\_Share** via your Device, you do not have to relogin unless you restart your computer.

## 3.7 Using the Media Server Feature

Use the media server feature to play files on a computer or on your television (using DMA-2500).

This section shows you how the media server feature works using the following media clients:

- Microsoft (MS) Windows Media Player

Media Server works with Windows Vista and Windows 7. Make sure your computer is able to play media files (music, videos and pictures).

- ZyXEL DMA-2500, a digital media adapter

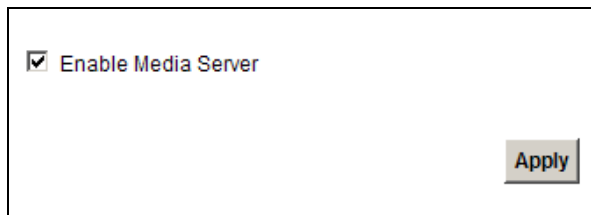
You need to set up the DMA-2500 to work with your television (TV). Refer to the DMA-2500 Quick Start Guide for the correct hardware connections.

Before you begin, connect the USB storage device containing the media files you want to play to the USB port of your Device.

### 3.7.1 Configuring the Device

Note: The Media Server feature is enabled by default.

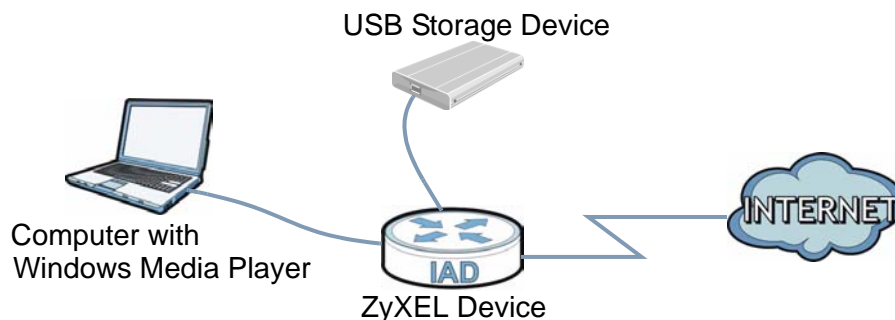
To use your Device as a media server, click **Network Setting > Home Networking > Media Server**.



Check **Enable Media Server** and click **Apply**. This enables DLNA-compliant media clients to play the video, music and image files in your USB storage device.

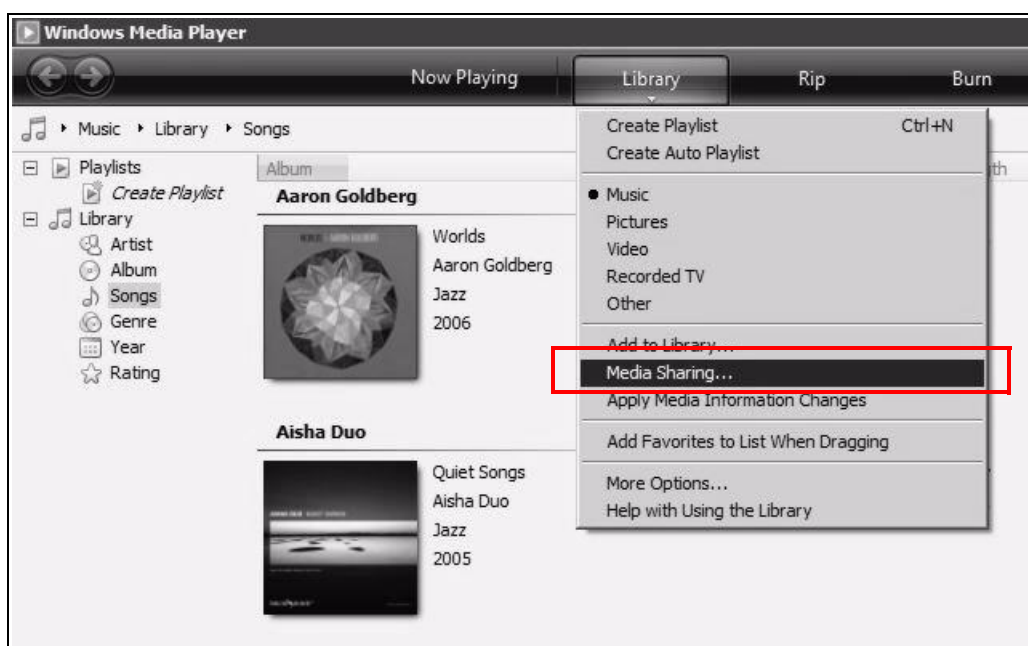
### 3.7.2 Using Windows Media Player

This section shows you how to play the media files on the USB storage device connected to your Device using Windows Media Player.

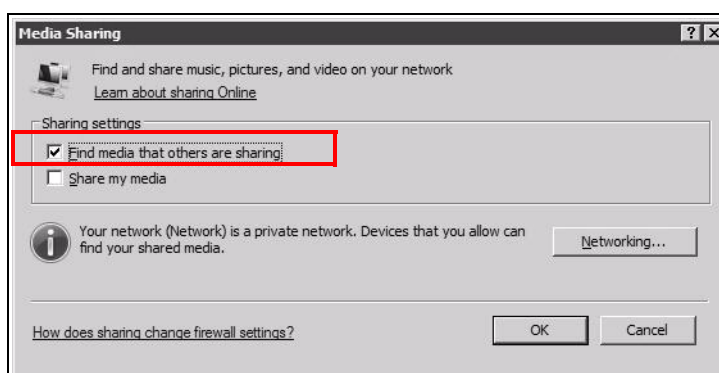


## Windows Vista

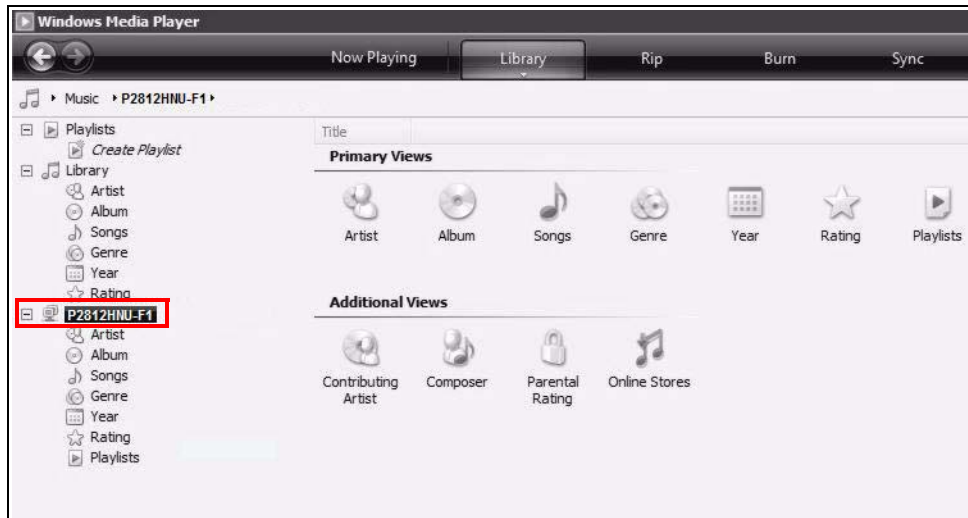
- 1 Open Windows Media Player and click **Library > Media Sharing** as follows.



- 2 Check **Find media that others are sharing** in the following screen and click **OK**.



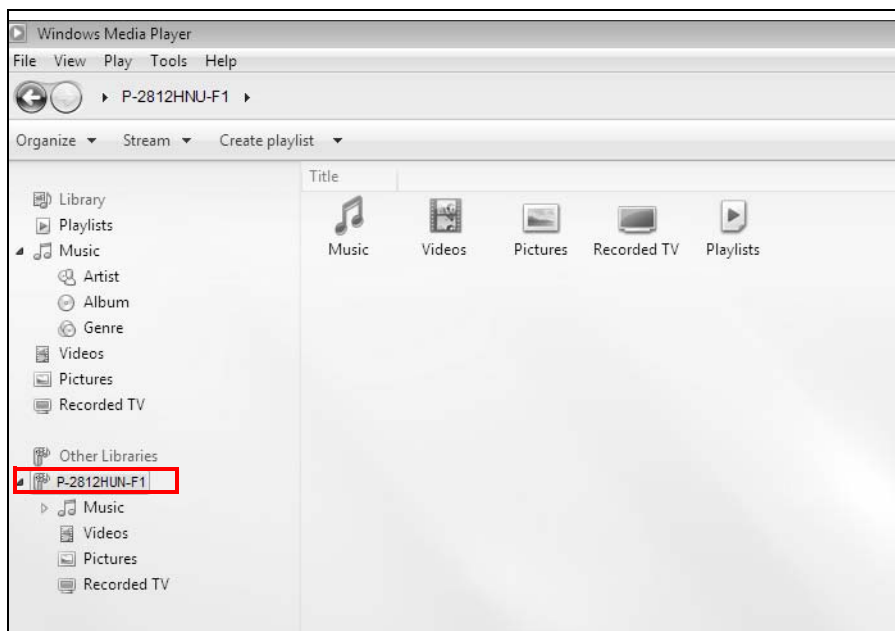
- 3 In the **Library** screen, check the left panel. The Windows Media Player should detect the Device.



The Device displays as a playlist. Clicking on the category icons in the right panel shows you the media files in the USB storage device attached to your Device.

## Windows 7

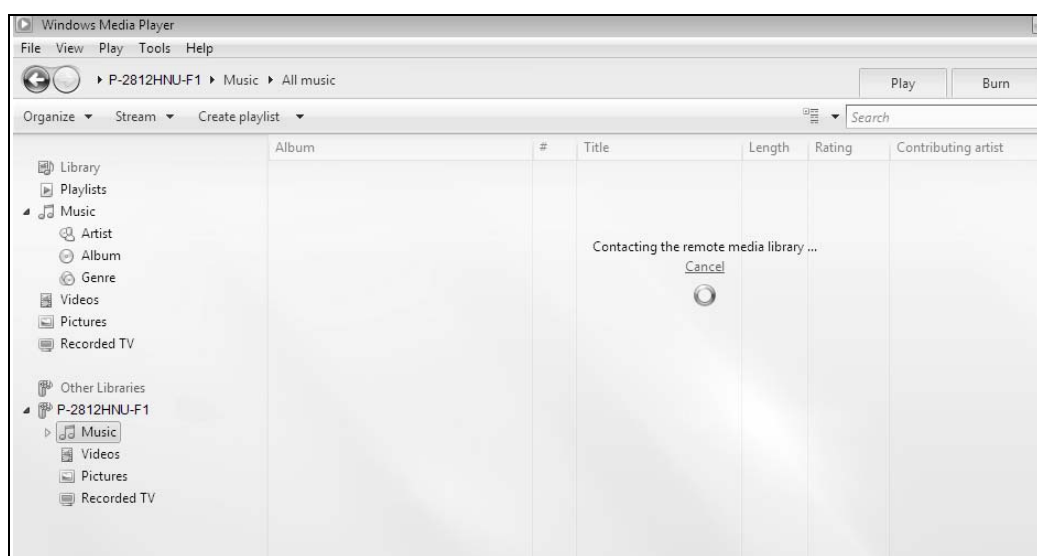
- 1 Open Windows Media Player. It should automatically detect the Device.



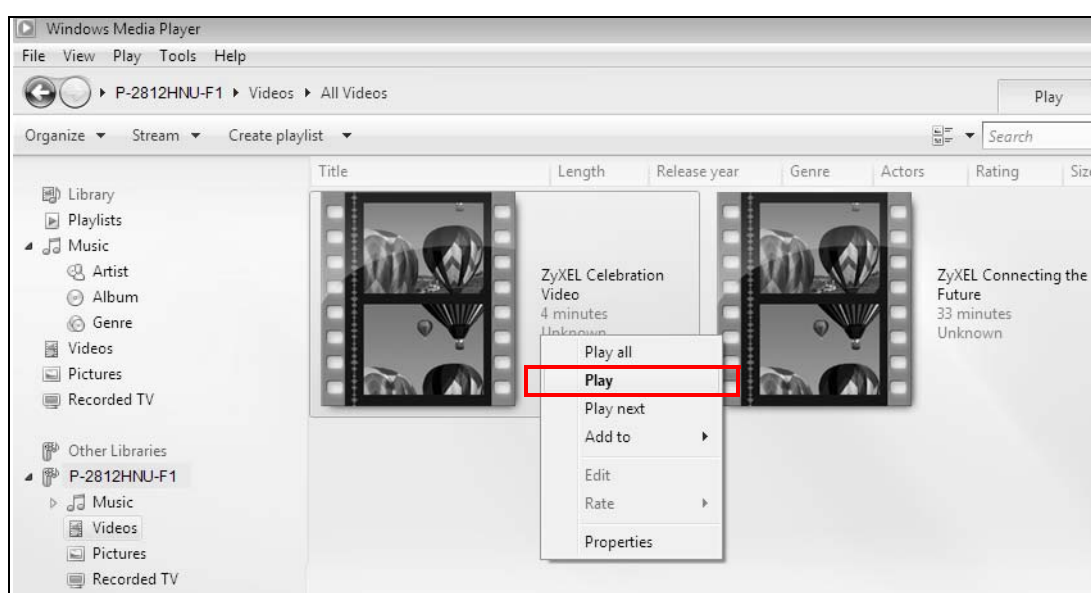
If you cannot see the Device in the left panel as shown above, right-click **Other Libraries** > **Refresh Other Libraries**.



- 2 Select a category in the left panel and wait for Windows Media Player to connect to the Device.



- 3 In the right panel, you should see a list of files available in the USB storage device.

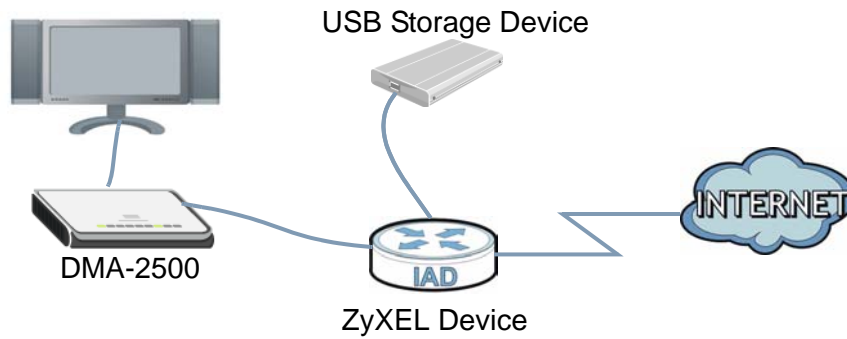


### 3.7.3 Using a Digital Media Adapter

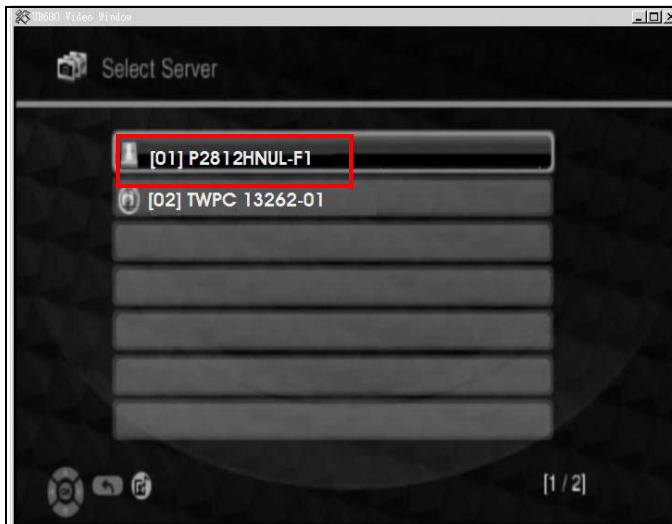
This section shows you how you can use the Device with a ZyXEL DMA-2500 to play media files stored in the USB storage device in your TV screen.

**Note:** For this tutorial, your DMA-2500 should already be set up with the TV according to the instructions in the DMA-2500 Quick Start Guide.

- 1 Connect the DMA-2500 to an available LAN port in your Device.



- 2 Turn on the TV and wait for the DMA-2500 **Home** screen to appear. Using the remote control, go to **MyMedia** to open the following screen. Select the Device as your media server.



- 3 The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button in the remote control.



## 3.8 Using the Print Server Feature

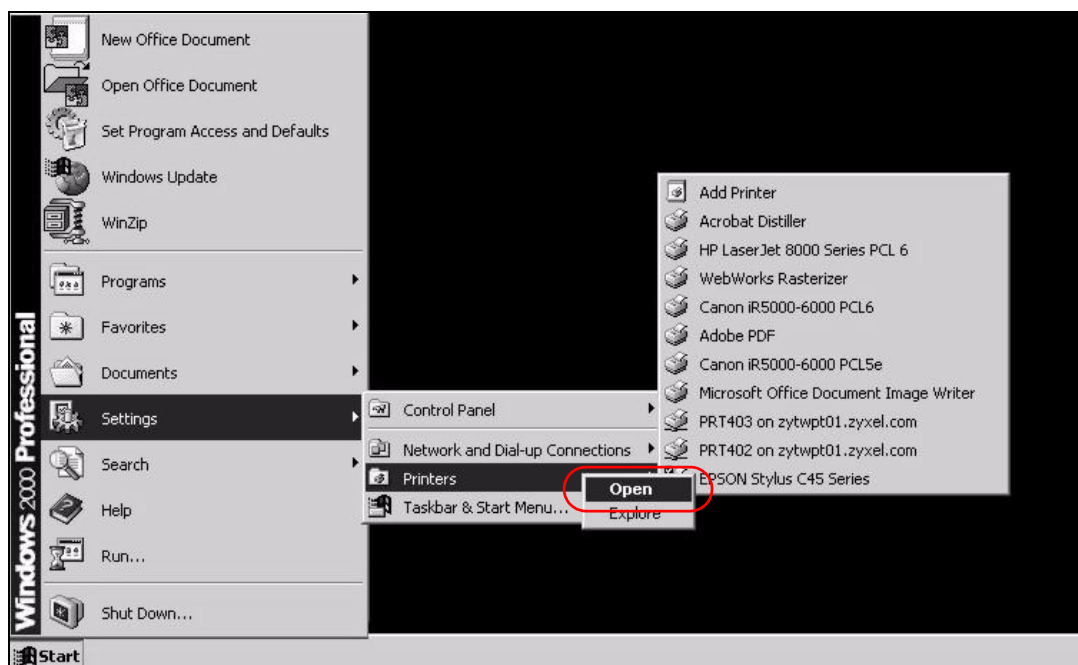
In this section you can:

- Configure a TCP/IP Printer Port
- Add a New Printer Using Windows
- Add a New Printer Using Macintosh OS X

### Configure a TCP/IP Printer Port

This example shows how you can configure a TCP/IP printer port. This example is done using the Windows 2000 Professional operating system. Some menu items may look different on your operating system. The TCP/IP port must be configured with the IP address of the Device and must use the RAW protocol to communicate with the printer. Consult your operating systems documentation for instructions on how to do this or follow the instructions below if you have a Windows 2000/XP operating system.

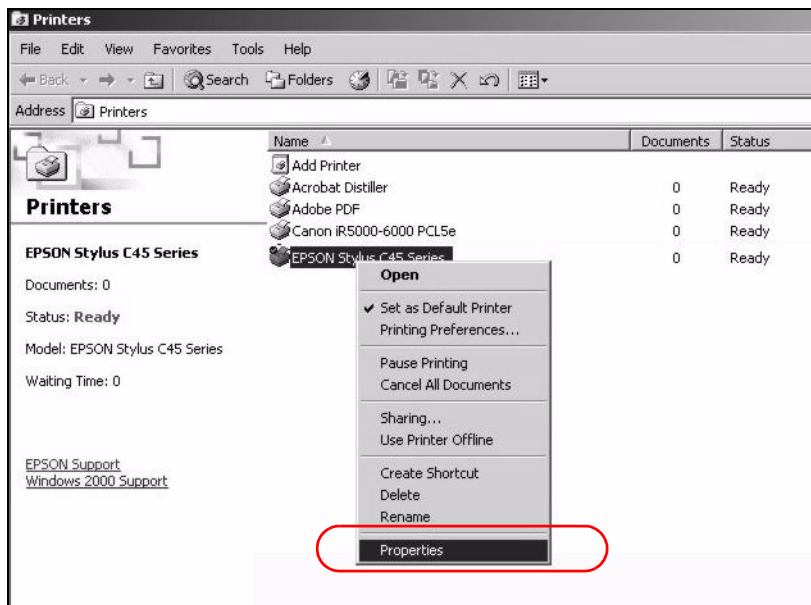
- 1 Click **Start > Settings**, then right click on **Printers** and select **Open**.



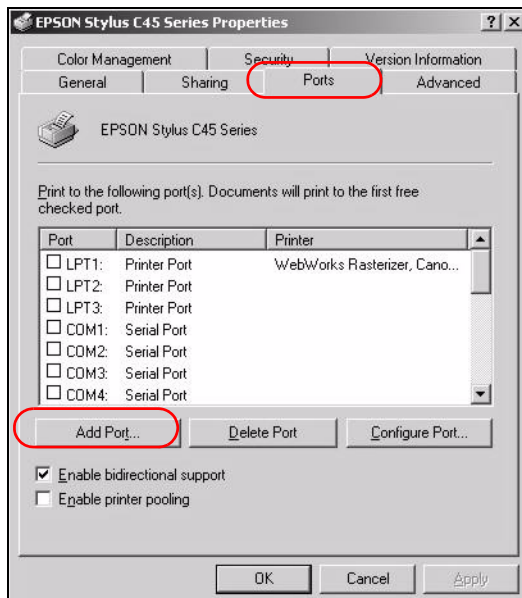
The **Printers** folder opens up. First you need to open up the properties windows for the printer you want to configure a TCP/IP port.

- 2 Locate your printer.

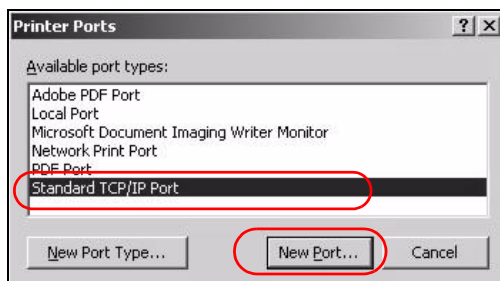
- 3 Right click on your printer and select **Properties**.



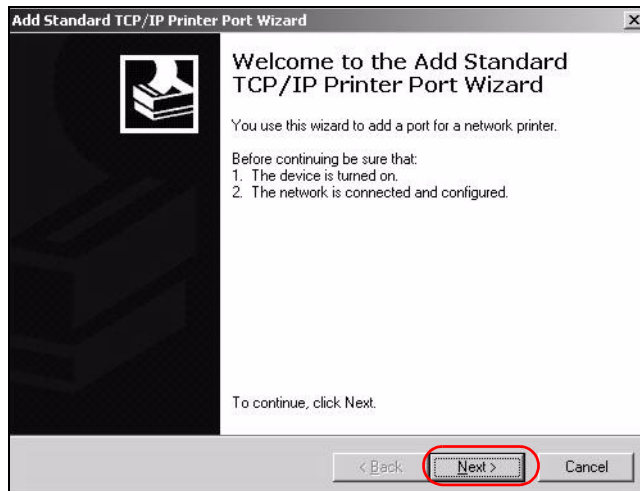
- 4 Select the **Ports** tab and click **Add Port...**



- 5 A **Printer Ports** window appears. Select **Standard TCP/IP Port** and click **New Port...**

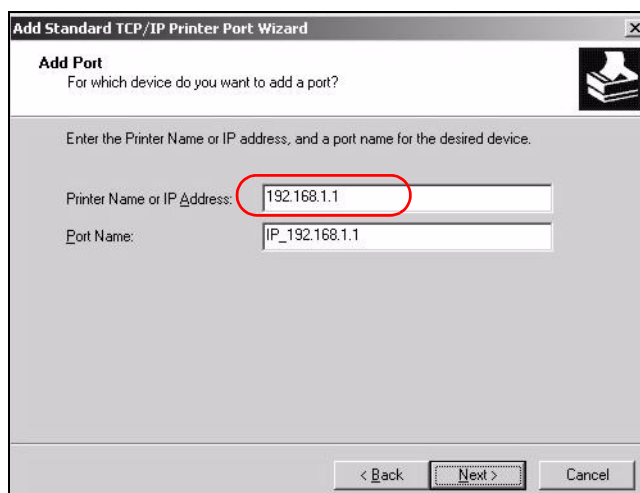


- 6 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

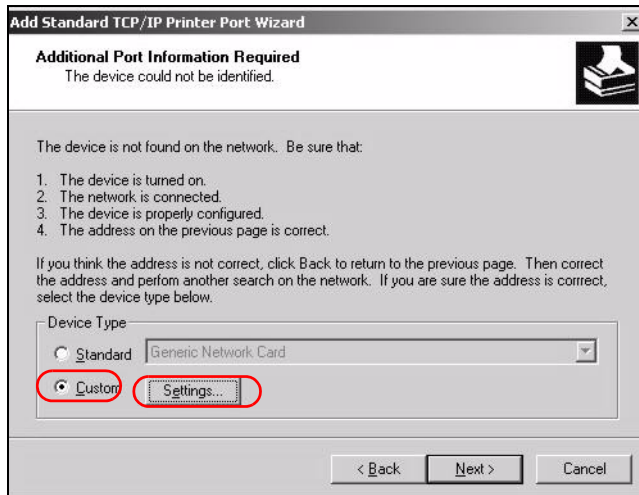


- 7 Enter the IP address of the Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.



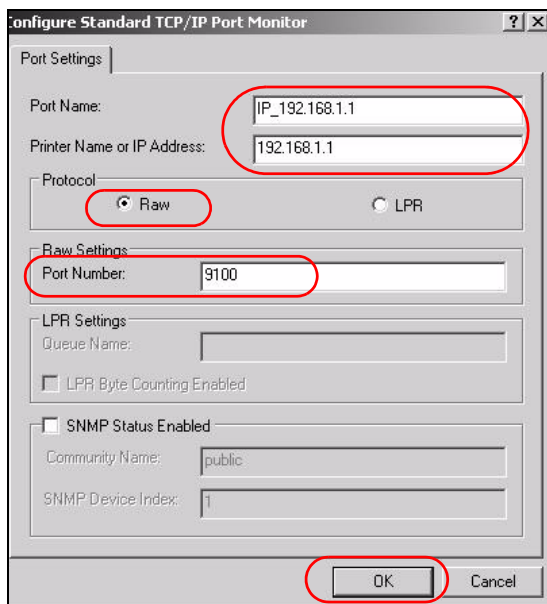
- 8 Select **Custom** under **Device Type** and click **Settings**.



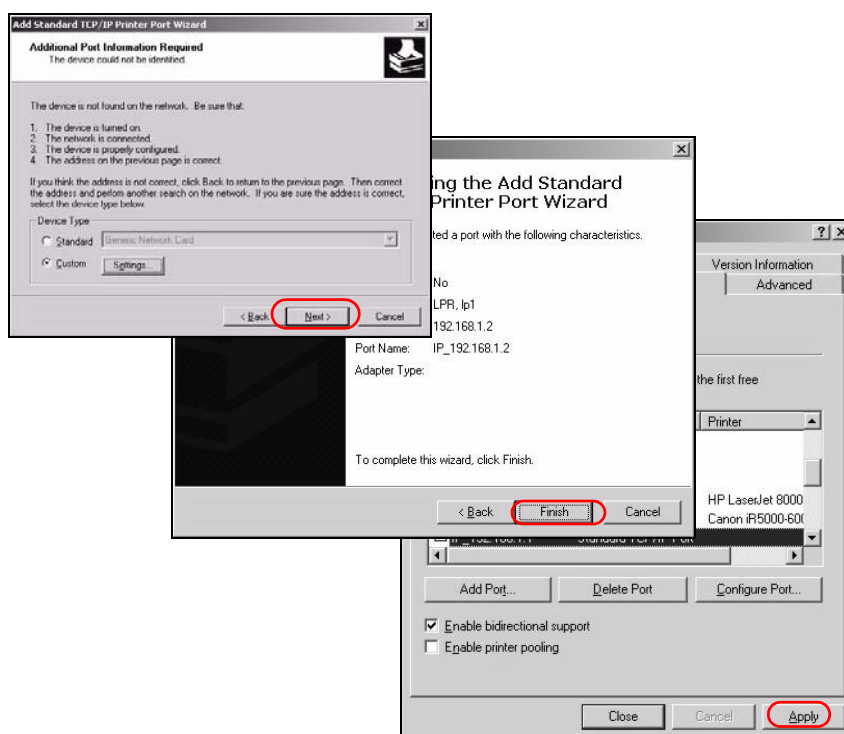
- 9 Confirm the IP address of the Device in the IP Address field.

- 10 Select **Raw** under **Protocol**.

- 11 The **Port Number** is automatically configured as **9100**. Click **OK**.



12 Continue through the wizard, apply your settings and close the wizard window.

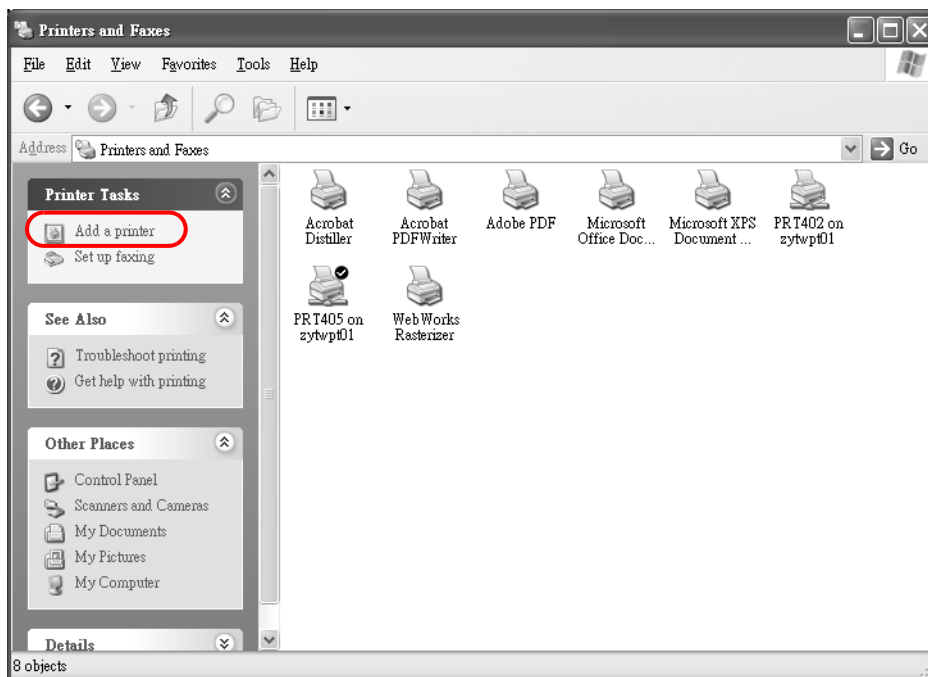


13 Repeat steps 1 to 12 to add this printer to other computers on your network.

## Add a New Printer Using Windows

This example shows how to connect a printer to your Device using the Windows XP Professional operating system. Some menu items may look different on your operating system.

- 1 Click **Start > Control Panel > Printers and Faxes** to open the **Printers and Faxes** screen. Click **Add a Printer**.

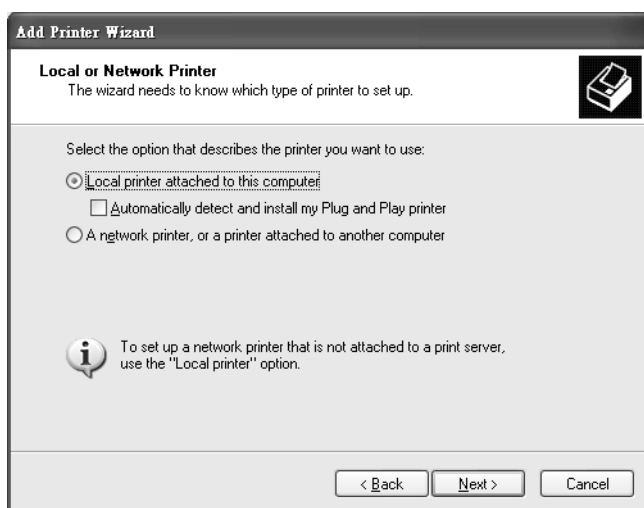


- 2 The **Add Printer Wizard** screen displays. Click **Next**.

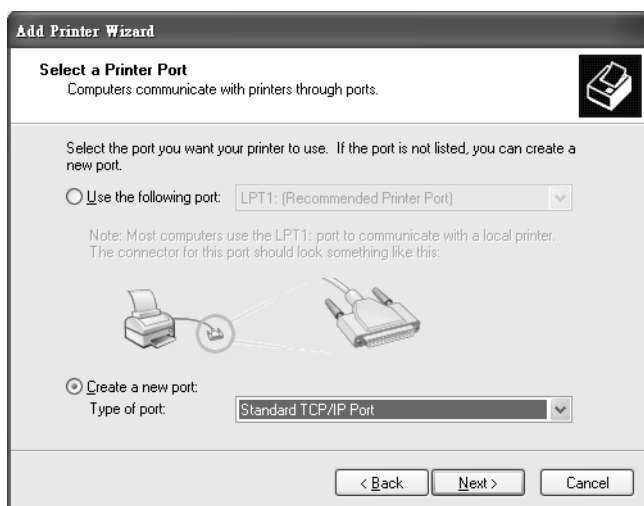




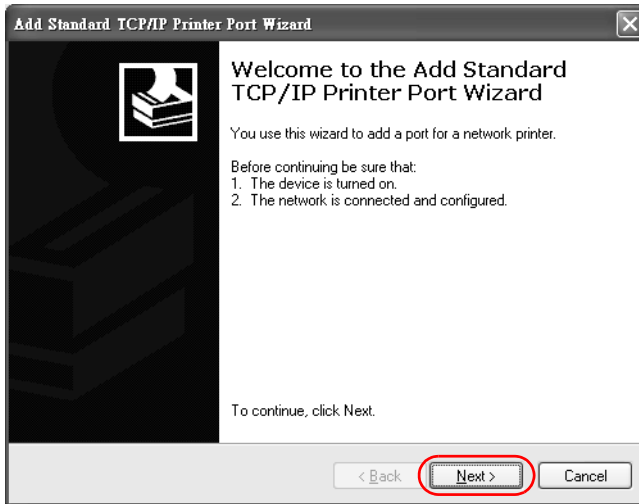
- 3 Select **Local printer attached to this computer** and click **Next**.



- 4 Select **Create a new port** and **Standard TCP/IP Port**. Click **Next**.

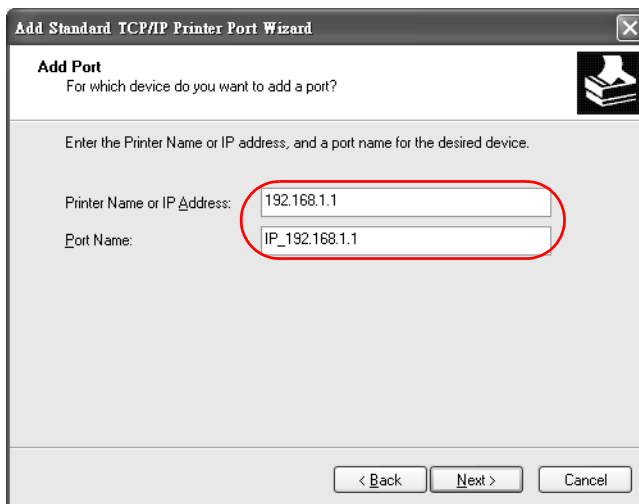


- 5 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

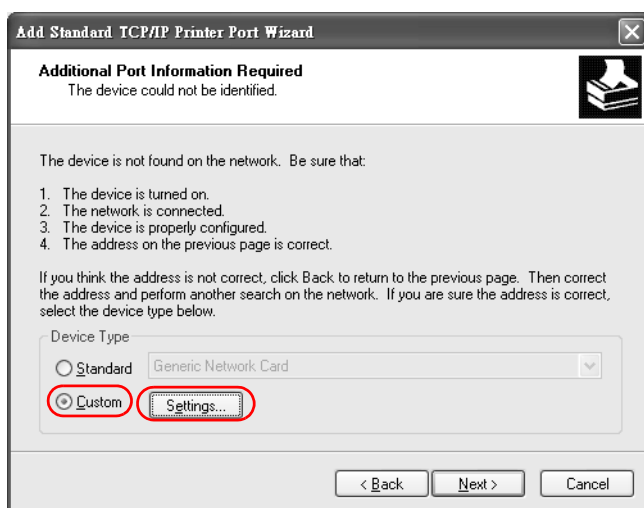


- 6 Enter the IP address of the Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

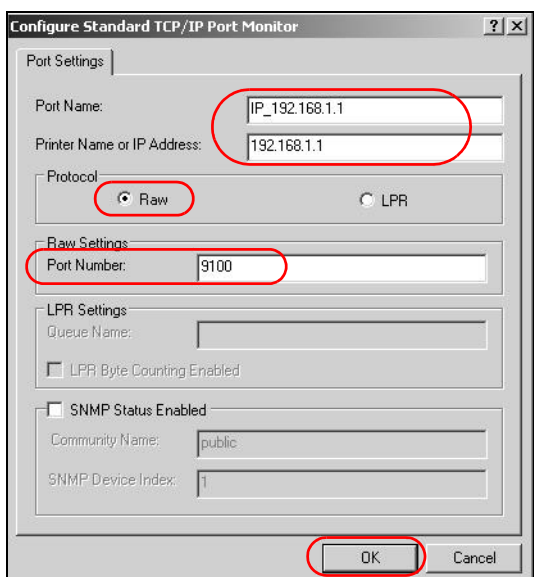
Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.



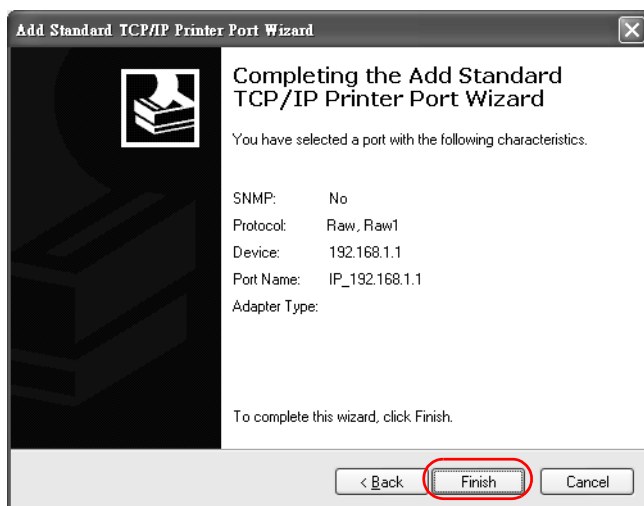
- 7 Select **Custom** under **Device Type** and click **Settings**.



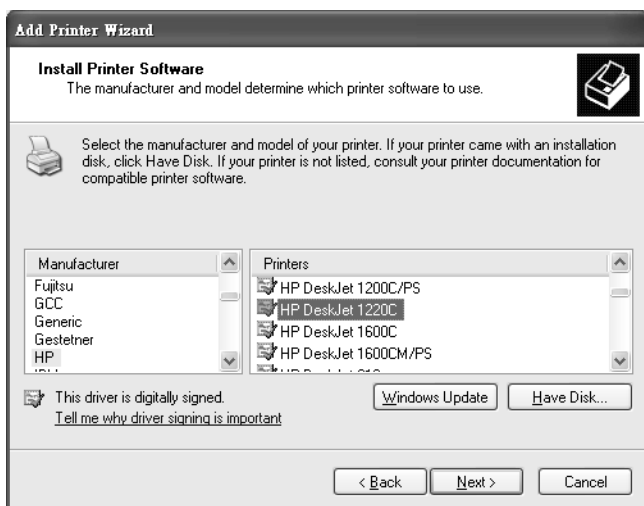
- 8 Confirm the IP address of the Device in the Printer **Name or IP Address** field.
- 9 Select **Raw** under **Protocol**.
- 10 The **Port Number** is automatically configured as **9100**. Click **OK** to go back to the previous screen and click **Next**.



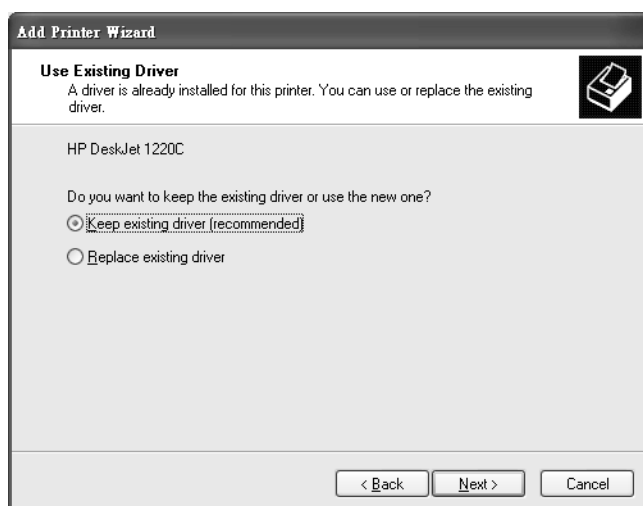
- 11 Click **Finish** to close the wizard window.



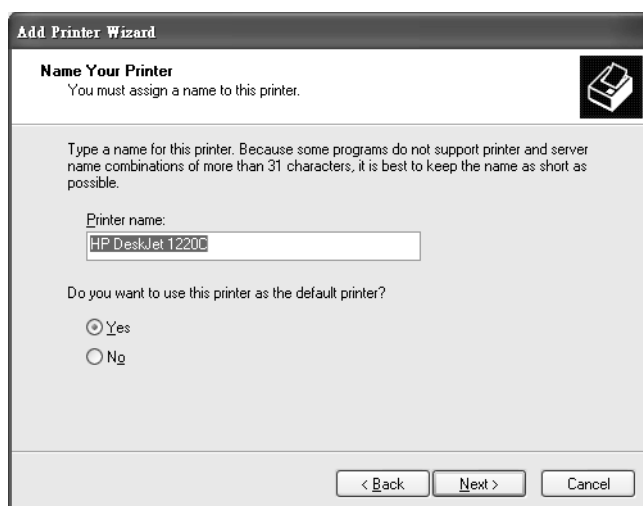
- 12 Select the make of the printer that you want to connect to the print server in the **Manufacturer** list of printers.
- 13 Select the printer model from the list of **Printers**.
- 14 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk...** and install the new printer driver.
- 15 Click **Next** to continue.



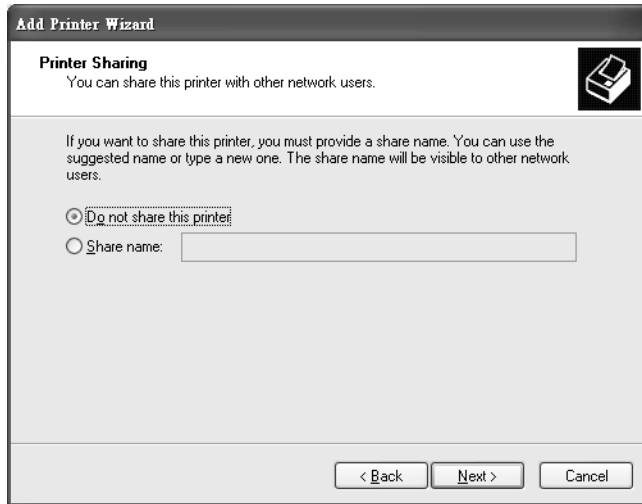
- 16 If the following screen displays, select **Keep existing driver** radio button and click **Next** if you already have a printer driver installed on your computer and you do not want to change it. Otherwise, select **Replace existing driver** to replace it with the new driver you selected in the previous screen and click **Next**.



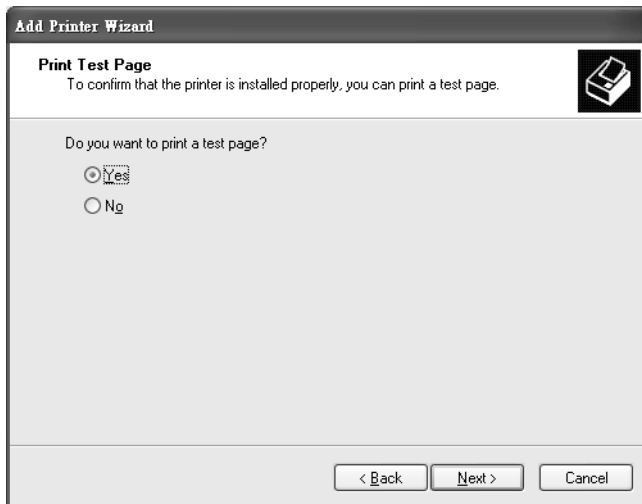
- 17 Type a name to identify the printer and then click **Next** to continue.



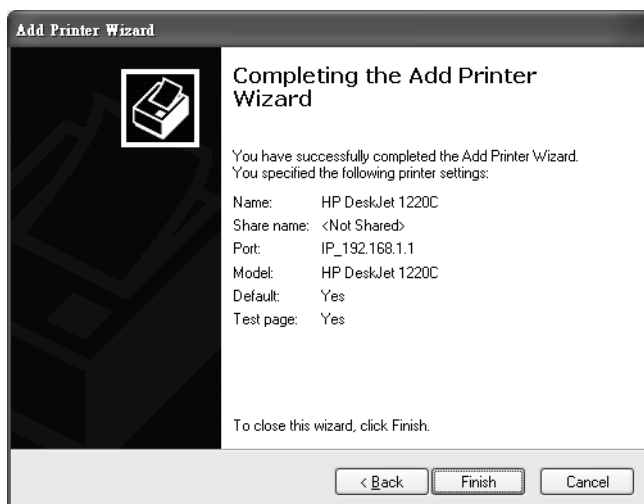
- 18 The Device is a print server itself and you do not need to have your computer act as a print server by sharing the printer with other users in the same network; just select **Do not share this printer** and click **Next** to proceed to the following screen.



- 19 Select **Yes** and then click the **Next** button if you want to print a test page. A pop-up screen displays to ask if the test page printed correctly. Otherwise select **No** and then click **Next** to continue.




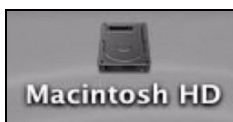
- 20 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.



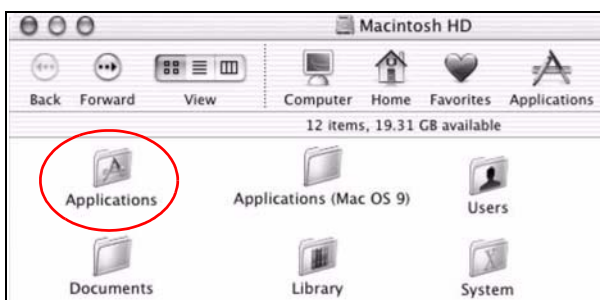
## Add a New Printer Using Macintosh OS X

Complete the following steps to set up a print server driver on your Macintosh computer.

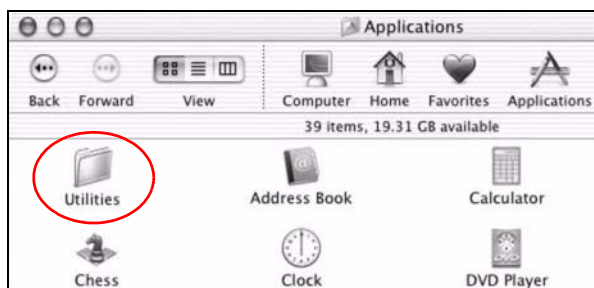
- 1 Click the **Print Center** icon  located in the Macintosh Dock (a place holding a series of icons/shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.
- 2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.



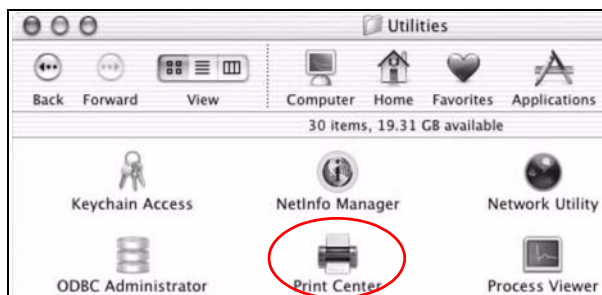
- 3 Double-click the **Applications** folder.



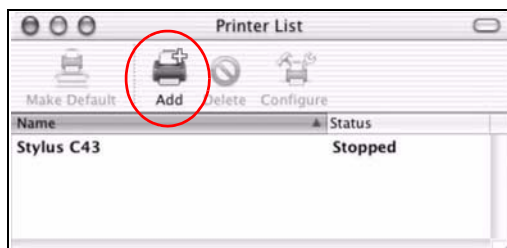
- 4 Double-click the **Utilities** folder.



- 5 Double-click the **Print Center** icon.



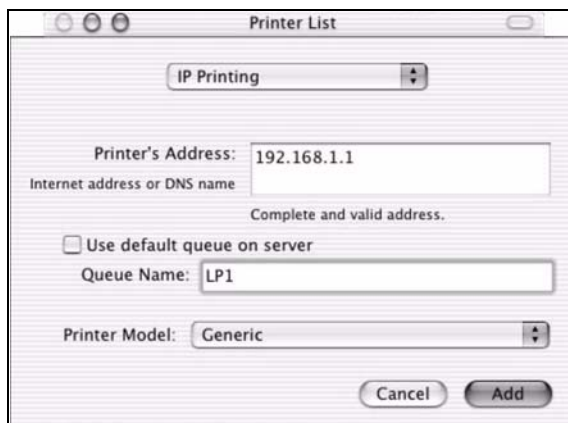
- 6 Click the **Add** icon at the top of the screen.



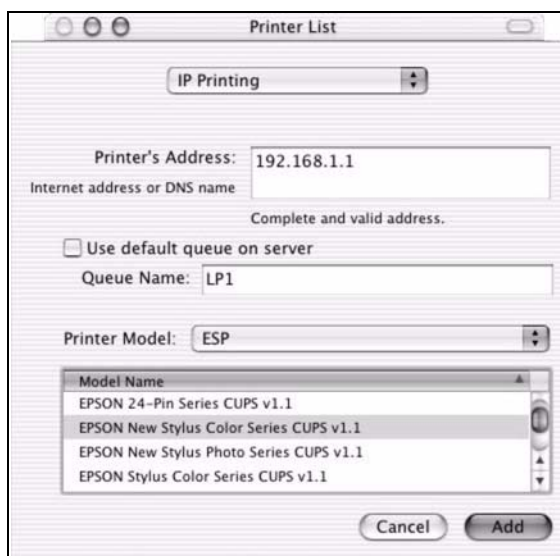
- 7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.
- 8 In the **Printer's Address** field, type the IP address of your Device.
- 9 Deselect the **Use default queue on server** check box.
- 10 Type **LP1** in the **Queue Name** field.



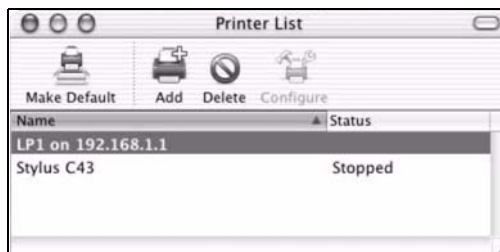
- 11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.



- 12 Click **Add** to select a printer model, save and close the **Printer List** configuration screen.



- 13 The **Name LP1 on 192.168.1.1** displays in the **Printer List** field. The default printer **Name** displays in bold type.

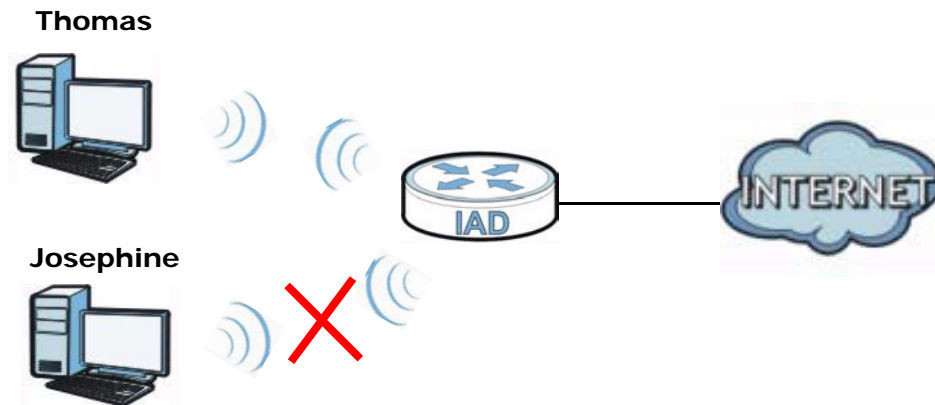


Your Macintosh print server driver setup is complete. You can now use the Device's print server to print from a Macintosh computer.

## 3.9 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



- 1 Click **Security > MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.
- 2 Find the MAC address of Thomas' computer in this screen. Select **Allow**. Click **Apply**.

MAC Address Filter: ☒ Enable ☐ Disable

Set	Allow	MAC Address
1	<input checked="" type="checkbox"/>	00:24:21:7E:20:96
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
30	<input type="checkbox"/>	
31	<input type="checkbox"/>	
32	<input type="checkbox"/>	

**Note:**  
Only devices listed here are granted access to the network.

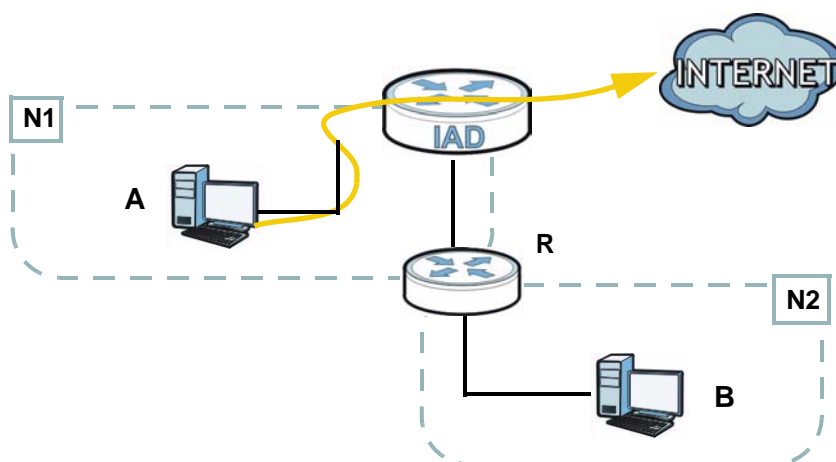
Apply Cancel

Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the Device.

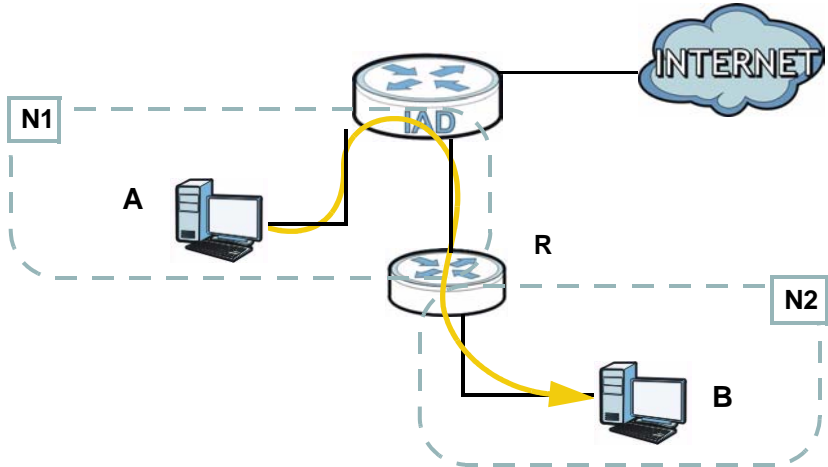
## 3.10 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**. This tutorial uses the following example IP settings:



**Table 3** IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The Device's WAN	172.16.1.1
The Device's LAN	192.168.1.1
<b>A</b>	192.168.1.34
<b>R</b> 's N1	192.168.1.253
<b>R</b> 's N2	192.168.10.2
<b>B</b>	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

- 1 Click **Network Setting > Routing**. Click **Add New Static Route**.

Add New Static Route									
#	Active	Status	MName	Destination IP	Gateway	Subnet Mask	Interface	Modify	

- 2 Configure the **Static Route Setup** screen using the following settings:
  - Select **Active**.
  - Specify a descriptive name for this routing rule.
  - Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

- Type **192.168.1.253** (R's N1 address) in the **Gateway IP Address** field.

☒ Active  
 Route Name :   
 Destination IP Address :   
 IP Subnet Mask :   
 Gateway IP Address :   
 Bound Interface ☐   
Apply Back

Click **Apply**. The **Routing** screen should display the route you just added.

Add New Static Route								
#	Active	Status	MName	Destination IP	Gateway	Subnet Mask	Interface	Modify
1			To_N2	192.168.10.0	192.168.1.253	255.255.255.0	LAN/br0	

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

## 3.11 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

**Note:** Voice traffic will not be affected by the user-defined QoS settings on the Device. It always gets the highest priority.

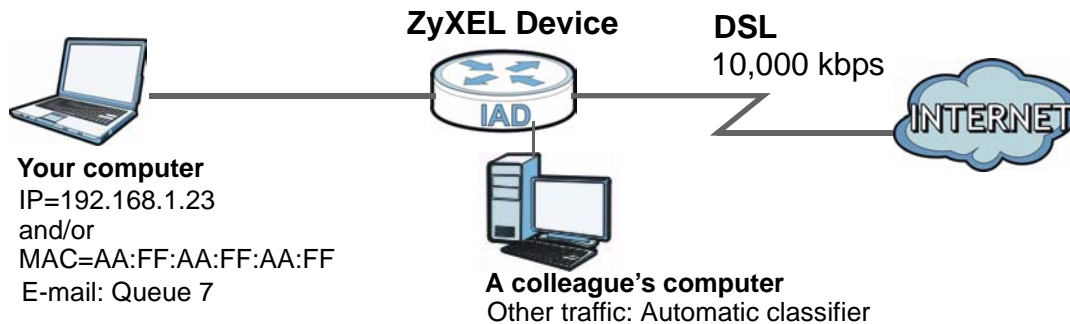
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

- Configure a queue to assign the highest priority queue (7) to e-mail traffic from the LAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the Device.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the Device.



- 1 Click **Network Setting > QoS > General** and check **Active**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Device automatically determine this figure). Click **Apply** to save your settings.

☒ Active QoS

WAN Managed Upstream Bandwidth : 10000 (kbps)

Traffic priority will be automatically assigned by: None

**Note :**  
You can assign the upstream bandwidth manually.  
If the field is empty, the CPE set the value automatically.  
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.

Apply Cancel

- 2 Go to **Network Setting > QoS > Queue Setup**. Click **Add new Queue** to create a new queue. In the screen that opens, check **Active** and enter or select the following values, then click **Apply**.

- **Name:** Email
- **Priority:** 7 (High)
- **Weight:** 15
- **Rate Limit:** 5,000 (kbps)

☒ Active

Name : Email

Interface : WAN

Priority : 7(High)

Weight : 15

Rate Limit : 5000 (kbps)

Apply Back

- 3 Go to **Network Setting > QoS > Class Setup**. Click **Add new Classifier** to create a new class. Check **Active** and follow the settings as shown in the screen below. Then click **Apply**.

**Class Configuration**

Active : ☒

Class Name : Email

Classification Order : 1

Forward To Interface : Unchange

DSCP Mark : Unchange (0-63)

802.1P : Mark : Unchange

To Queue : Email

**Criteria Configuration**  
Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

▪ Basic

☒ From Interface : Lan

☒ Ether Type : IP (0x0800)

▪ Source

☒ MAC Address : AA:FF:AA:FF:AA:FF MAC Mask :  ☐ Exclude

☒ IP Address : 192.168.1.23 IP Subnet Mask : 255.255.255.0 ☐ Exclude

☐ Port Range :  ~  (1-65535) ☐ Exclude

▪ Destination

☐ MAC Address :  MAC Mask :  ☐ Exclude

☐ IP Address :  IP Subnet Mask :  ☐ Exclude

☐ Port Range :  ~  (1-65535) ☐ Exclude

▪ Others

☐ 802.1P : 0 BE ☐ Exclude

☒ IP Protocol : User defined 25 ☐ Exclude

☐ IP Packet Length :  ~  (46-1504) ☐ Exclude

☐ DSCP :  ☐ Exclude

☐ TCP ACK ☐ Exclude

☐ DHCP : VendorClassID (DHCP Option 60)  ☐ Exclude

Class ID :  (String)

☐ Service : FTP ☐ Exclude

Apply Back

<b>Class Name</b>	Give a class name to this traffic, such as <b>Email</b> in this example.
<b>To Queue</b>	Link this to a queue created in the <b>QoS &gt; Queue Setup</b> screen, which is the <b>Email</b> queue created in this example.
<b>From Interface</b>	This is the interface from which the traffic will be coming from. Select <b>Lan</b> .
<b>Ether Type</b>	Select <b>IP</b> to identify the traffic source by its IP address or MAC address.
<b>MAC Address</b>	Type the MAC address of your computer - <b>AA:FF:AA:FF:AA:FF</b> . Type the <b>MAC Mask</b> if you know it.
<b>IP Address</b>	Type the IP address of your computer - <b>192.168.1.23</b> . Type the <b>IP Subnet Mask</b> if you know it.
<b>IP Protocol</b>	Select <b>User defined</b> and enter <b>25</b> as the IP Protocol.

This maps e-mail traffic to queue 7 created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to queue 7 (see the **Source** fields).

- 4 Verify that the queue setup works by checking **Network Setting > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.

**Monitor**  
Refresh Interval :

**Status :**

▪ Interface Monitor

#	Name	Pass Rate(bps)
1	ptm0.3900	

▪ Queue Monitor

#	Name	Interface	Pass Rate(bps)	Drop Rate(bps)
1	WAN_Default_Queue	WAN	0	0
2	LAN_Default_Queue	LAN	0	0
3	Fast	WAN	0	0
4	Active user	WAN	0	0
5	Passive user	WAN	0	0
6	Slow	WAN	0	0
7	Email	WAN	2992	0

## 3.12 Access the Device Using DDNS

If you connect your Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Device using a domain name.



To use this feature, you have to apply for DDNS service at [www.dyndns.org](http://www.dyndns.org).

This tutorial shows you how to:

- [Registering a DDNS Account on \[www.dyndns.org\]\(http://www.dyndns.org\)](#)
- [Configuring DDNS on Your Device](#)
- [Testing the DDNS Setting](#)

Note: If you have a private WAN IP address, then you cannot use DDNS.



### 3.12.1 Registering a DDNS Account on www.dyndns.org

- 1 Open a browser and type **http://www.dyndns.org**.
- 2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
- 3 Log into www.dyndns.org using your account.
- 4 Add a new DDNS host name. This tutorial uses the following settings as an example.
  - Hostname: **zyxelrouter.dyndns.org**
  - Service Type: **Host with IP address**
  - IP Address: Enter the WAN IP address that your Device is currently using. You can find the IP address on the Device's web configurator **Status** page.

Then you will need to configure the same account and host name on the Device later.

### 3.12.2 Configuring DDNS on Your Device

Configure the following settings in the **Network Setting > Dynamic DNS** screen.

- Select **Active Dynamic DNS**.
- Select **Dynamic DNS** for the DDNS type.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).

**Dynamic DNS Configuration**

☒ Active Dynamic DNS

Service Provider :

Dynamic DNS Type :

Host Name :  (1 to 255 characters)

User Name :  (1 to 255 characters)

Password :  (1 to 63 characters)

Click **Apply**.

### 3.12.3 Testing the DDNS Setting

Now you should be able to access the Device from the Internet. To test this:

- 1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
- 2 Type **http://zyxelrouter.dyndns.org** and press [Enter].
- 3 The Device's login page should appear. You can then log into the Device and manage it.



---

# PART II

## Technical Reference

---

The appendices provide general information. Some details may not apply to your NWA.



# Connection Status and System Info

## 4.1 Overview

After you log into the web configurator, the **Connection Status** screen appears. This shows the network connection status of the Device and clients connected to it.

Use the **System Info** screen to look at the current status of the device, system resources, interfaces (LAN, WAN and WLAN), and SIP accounts. You can also register and unregister SIP accounts.

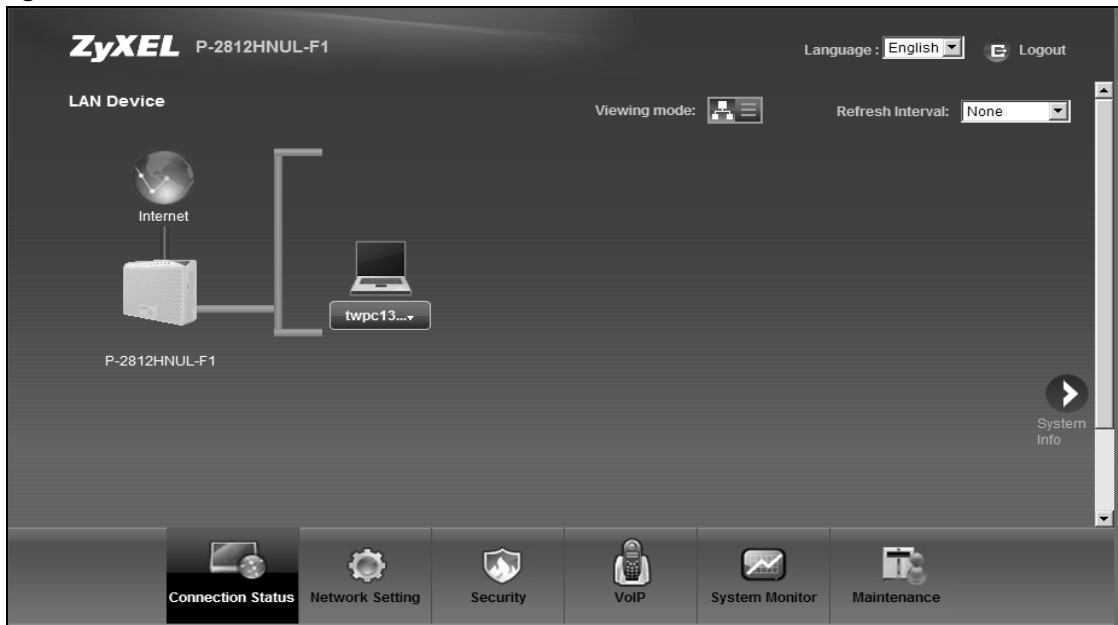
If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the Device's ports. See [Section 2.2.2 on page 29](#) for more information.

## 4.2 The Connection Status Screen

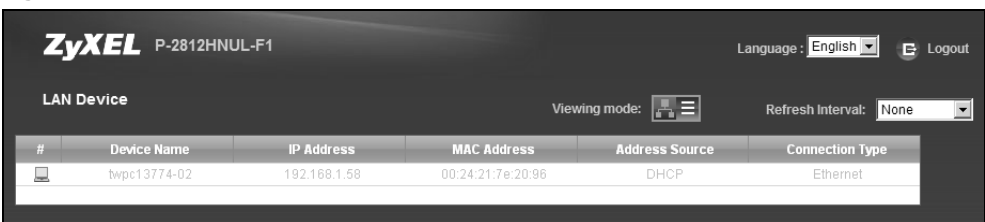
Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

If you prefer to view the status in a list, click **List View** in the **Viewing mode** selection box. You can configure how often you want the Device to update this screen in **Refresh Interval**.

**Figure 10** Connection Status: Icon View



**Figure 11** Connection Status: List View



In **Icon View**, if you want to view information about a client, click the client's name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change name/icon**.

In **List View**, you can also view the client's information.

## 4.3 The System Info Screen

Click **Connection Status > System Info** to open this screen.

**Figure 12** System Info Screen

**ZyXEL P-2812HNUL-F1** Language: English Logout

System Info Refresh Interval: None

Device Information	
Host Name:	router
Model Name:	P-2812HNUL-F1
MAC Address:	00:13:49:11:66:8f
Firmware Version:	V3.10(TUJ.0)b4
WAN 1 Information:	(VDSL WAN 1)
- Mode:	IPoE
- IP Address:	
- IP Subnet Mask:	
LAN Information:	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP Server:	Server
- DHCPv6 Server:	DHCPv6 Relay
WLAN Information:	
- Channel:	11
- WPS Status:	Unconfigured
SSID1 Information:	
- SSID:	ZyXEL_668C
- Status:	On
- Security Mode:	WPA2-PSK mixed
SSID2 Information:	
- SSID:	ZyXEL_668D
- Status:	Off
- Security Mode:	WPA2-PSK mixed
SSID3 Information:	
- SSID:	ZyXEL_668E
- Status:	Off
- Security Mode:	WPA2-PSK mixed
SSID4 Information:	
- SSID:	ZyXEL_668F
- Status:	Off
- Security Mode:	WPA2-PSK mixed

Interface Status		
Interface	Status	Rate
VDSL WAN	Down	N/A
LAN 1	Up	1000Mbps
LAN 2	Down	N/A
LAN 3	Down	N/A
LAN 4	Down	N/A
WLAN	Up	300Mbps
3G	Disabled	N/A

System Status	
DSL Up Time:	N/A
System Up Time:	1 day, 6:19
Current Date/Time:	Sun Jan 2 07:19:54 CET 2000
System Resource:	
- CPU Usage:	2.0%
- Memory Usage:	51.8%

USB Status	
Type	Status
Storage	N/A
Printer	N/A

Registration Status			
Account	Action	Account Status	URI
SIP 1	Register	In-Active	ChangeMe@ChangeMe
SIP 2	Register	In-Active	ChangeMe@ChangeMe

Each field is described in the following table.

**Table 4** System Info Screen

LABEL	DESCRIPTION
Language	Select the web configurator language from the drop-down list box.
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Device Information	
Host Name	This field displays the Device system name. It is used for identification. You can change this in the <b>Maintenance &gt; System</b> screen's <b>Host Name</b> field.
Model Name	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Device.

**Table 4** System Info Screen (continued)

LABEL	DESCRIPTION
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Go to the <b>Maintenance &gt; Firmware Upgrade</b> screen to change it.
WAN Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the Device in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP Server	<p>This field displays what DHCP services the Device is providing to the LAN. Choices are:</p> <p><b>Server</b> - The Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p><b>None</b> - The Device is not providing any DHCP services to the LAN.</p>
DHCPv6 Server	<p>This field displays what DHCPv6 services the Device is providing to the LAN. Choices are:</p> <p><b>Server</b> - The Device is a DHCPv6 server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p><b>Relay</b> - The Device acts as a surrogate DHCPv6 server and relays DHCP requests and responses between the remote server and the clients.</p> <p><b>None</b> - The Device is not providing any DHCPv6 services to the LAN.</p>
WLAN Information	
Channel	This is the channel number used by the Device now.
WPS Status	<b>Configured</b> displays when a wireless client has connected to the Device or WPS is enabled and wireless or wireless security settings have been configured. <b>Unconfigured</b> displays if WPS is disabled or wireless security settings have not been configured.
SSID (1~4) Information	
SSID	This is the descriptive name used to identify the Device in the wireless LAN.
Status	This shows whether or not the SSID is enabled (on).
Security Mode	This displays the type of security the Device is using in the wireless LAN.
Interface Status	
Interface	This column displays each interface the Device has.



**Table 4** System Info Screen (continued)

LABEL	DESCRIPTION
Status	<p>This field indicates whether or not the Device is using the interface.</p> <p>For the DSL interface, this field displays <b>Down</b> (line is down), <b>Up</b> (line is up or connected) if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Up</b> (line is up or connected), <b>Idle</b> (line ppp idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation.</p> <p>For the WAN interface, this field displays <b>Up</b> when the Device is using the interface and <b>Down</b> when the Device is not using the interface.</p> <p>For the LAN interface, this field displays <b>Up</b> when the Device is using the interface and <b>Down</b> when the Device is not using the interface.</p> <p>For the WLAN interface, it displays <b>Active</b> when WLAN is enabled or <b>InActive</b> when WLAN is disabled.</p> <p>For the 3G interface, it displays <b>Enabled</b> when 3G is enabled or <b>Disabled</b> when 3G is disabled.</p>
Rate	<p>For the LAN interface, this displays the port speed and duplex setting.</p> <p>For the WAN interface, this displays the port speed and duplex setting.</p> <p>For the DSL interface, it displays the downstream and upstream transmission rate.</p> <p>For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or <b>N/A</b> when WLAN is disabled.</p> <p>For the 3G interface, it displays the maximum transmission rate when 3G is enabled or <b>N/A</b> when 3G is disabled.</p>
System Status	
DSL Up Time	This field displays how long the DSL connection has been active.
System Up Time	This field displays how long the Device has been running since it last started up. The Device starts up when you plug it in, when you restart it ( <b>Maintenance &gt; Reboot</b> ), or when you reset it (see <a href="#">Section 1.7 on page 26</a> ).
Current Date/Time	This field displays the current date and time in the Device. You can change this in <b>Maintenance &gt; Time Setting</b> .
System Resource	
CPU Usage	This field displays what percentage of the Device's processing ability is currently used. When this percentage is close to 100%, the Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
Memory Usage	This field displays what percentage of the Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the Device is probably becoming unstable, and you should restart the device. See <a href="#">Chapter 25 on page 267</a> , or turn off the device (unplug the power) for a few seconds.
USB Status	
Type	This shows the type of device connected to the Device.
Status	This shows whether the device is currently active ( <b>Up</b> ). This shows <b>N/A</b> if there are no device connected to the Device or the connected device is not working.
Registration Status	
Account	This column displays each SIP account in the Device.

**Table 4** System Info Screen (continued)

LABEL	DESCRIPTION
Action	<p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p>If the SIP account is already registered with the SIP server,</p> <ul style="list-style-type: none"> <li>Click <b>Unregister</b> to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name.</li> <li>The second field displays <b>Registered</b>.</li> </ul> <p>If the SIP account is not registered with the SIP server,</p> <ul style="list-style-type: none"> <li>Click <b>Register</b> to have the Device attempt to register the SIP account with the SIP server.</li> <li>The second field displays the reason the account is not registered.</li> </ul> <p><b>Inactive</b> - The SIP account is not active. You can activate it in <b>VoIP &gt; SIP &gt; SIP Settings</b>.</p> <p><b>Register Fail</b> - The last time the Device tried to register the SIP account with the SIP server, the attempt failed. The Device automatically tries to register the SIP account when you turn on the Device or when you activate it.</p>
Account Status	<p>This shows <b>Active</b> when the SIP account has been registered and ready for use or <b>In-Active</b> when the SIP account is not yet registered.</p>
URI	<p>This field displays the account number and service domain of the SIP account. You can change these in <b>VoIP &gt; SIP &gt; SIP Settings</b>.</p>

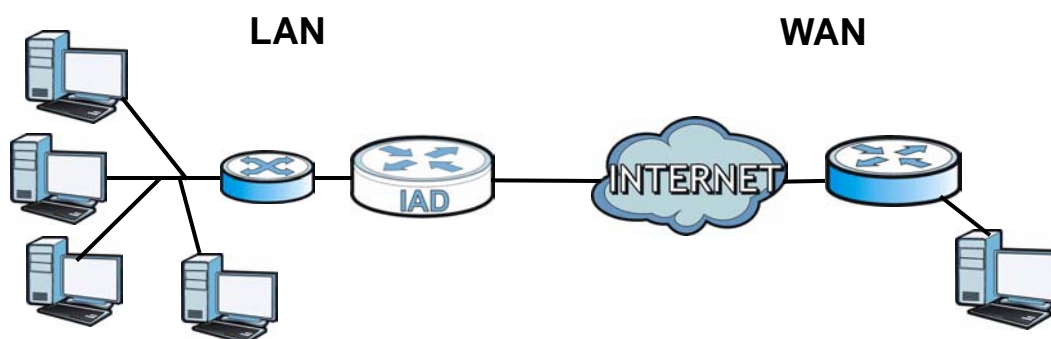
# Broadband

## 5.1 Overview

This chapter discusses the Device's **Broadband** screens. Use these screens to configure your Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

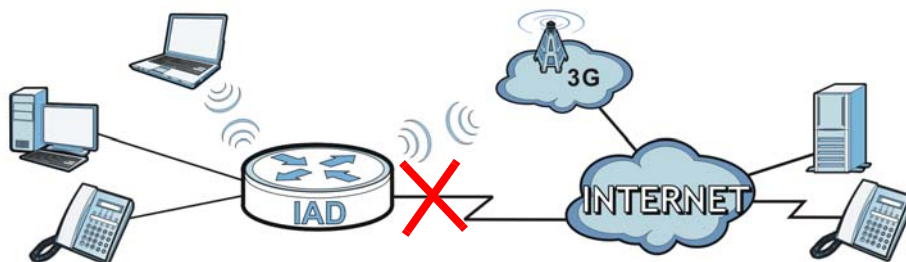
**Figure 13** LAN and WAN



3G (third generation) standards for the sending and receiving of voice, video, and data in a mobile environment.

You can attach a 3G wireless adapter to the USB port and set the Device to use this 3G connection as your WAN or a backup when the wired WAN connection fails.

**Figure 14** 3G WAN Connection



## 5.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the ZyXEL Device for Internet access ([Section 5.2 on page 91](#)).
- Use the **3G Backup** screen to configure 3G WAN connection ([Section 5.3 on page 115](#)).

**Table 5** WAN Setup Overview

LAYER-2 INTERFACE		INTERNET CONNECTION		
INTERFACE	DSL LINK TYPE	MODE	WAN SERVICE TYPE	CONNECTION SETTINGS
VDSL		Routing	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
		Bridge	N/A	N/A
ADSL	EoA	Routing	PPPoE/PPPOA	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
		Bridge	N/A	N/A
EtherWAN		Routing	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
		Bridge	N/A	N/A

## 5.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

### Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

### WAN IP Address

The WAN IP address is an IP address for the Device, which makes it accessible from an outside network. It is used by the Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

## ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between Finding Out More

## PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

## 3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

## IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to  $3.4 \times 10^{38}$  IP addresses. The Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

## IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So  
2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as  
2001:db8:1a2b:15:0:0:1a2f:0.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So  
2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as  
2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015,  
2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.

## IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

2001:db8:1a2b:15::1a2f:0/32

means that the first 32 bits (2001:db8) is the subnet prefix.

## IPv6 Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

## DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique Identifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

## IPv6 6to4 Mode

This mode also enables the Device to convert IPv6 packets to IPv4 packets. But instead of pre-configuring the destination router, you need to configure a 6to4 relay router that helps to route the packets to any IPv6 networks.

In this mode, the Device should get a public IPv4 address for the WAN. The Device adds an IPv4 header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the Device removes the IPv4 header from an IPv6 packet when receiving it from the Internet.

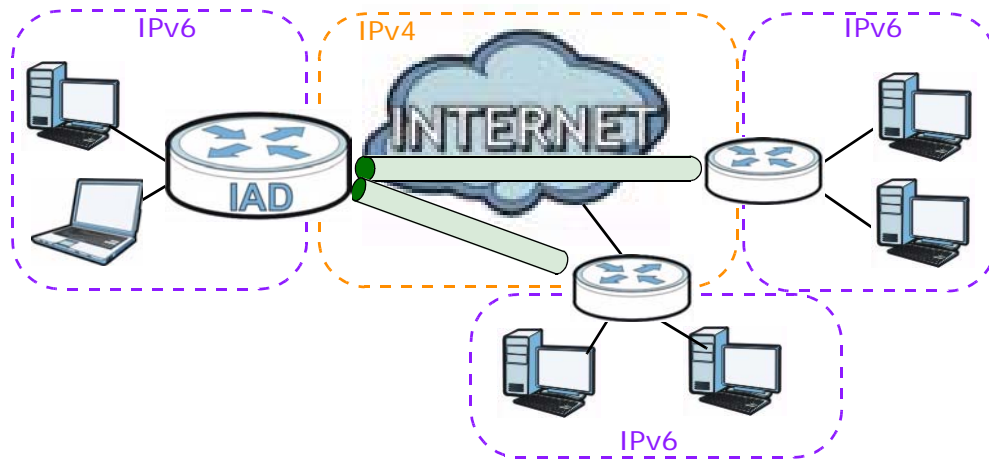
An IPv6 address using the 6to4 mode consists of an IPv4 address, the format is as the following:

2002:[a public IPv4 address in hexadecimal]::/48

For example,

A public IPv4 address is 202.156.30.41. The converted hexadecimal IP string is ca.9c.1E.29. The IPv6 address prefix becomes 2002:ca9c:1e29::/48.

**Figure 15** IPv6 6to4 Mode



### Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Device passes the IPv6 prefix information to LAN hosts. The hosts use the prefix to generate their IPv6 addresses.

### 5.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

## 5.2 The Broadband Screen

The Device must have a WAN interface to allow users to use the Ethernet WAN port or DSL port to access the Internet. Use the **Broadband** screen to view or modify a WAN interface.

Click **Network Setting > Broadband**. The following screen opens.

**Figure 16** Network Setting > Broadband

**Switch WAN Mode**

Type: VDSL Switch WAN Interface

Add new WAN Interface

**Internet Setup**

#	Name	Type	Mode	Encapsula...	IPv6	VPI	VCI	Vlan8021p
1	EtherWAN1	EtherWAN	Routing	IPoE	Disable	N/A	N/A	N/A
2	AdslWAN1	ADSL	Routing	IPoE	Disable	8	35	N/A
3	VdslWAN1	VDSL	Routing	IPoE	Disable	N/A	N/A	N/A

VlanMuxId	ATM QoS	IGMP Proxy	NAT	Default Gat...	Modify
N/A	N/A	Enabled	Enabled	Yes	
N/A	UBR	Enabled	Enabled	Yes	
N/A	N/A	Enabled	Enabled	Yes	

The following table describes the fields in this screen.

**Table 6** Network Setting > Broadband

LABEL	DESCRIPTION
Switch WAN Mode	
Type	If you prefer not to use a DSL line and you have another broadband modem or router (such as ADSL) available, you can select <b>EtherWAN</b> from the drop-down list box and click <b>Switch WAN Interface</b> . The Device will use Ethernet WAN as the WAN mode.
Add new WAN Interface	Click this to create a new WAN interface.
#	This is the index number of the connection.
Name	This is the service name of the connection.
Type	This shows the type of interface used by this connection.
Mode	This shows whether the connection is in routing mode or bridge mode.
Encapsulation	This shows the method of encapsulation used by this connection.
IPv6	This shows whether IPv6 is enabled.
VPI	This is the Virtual Path Identifier (VPI).
VCI	This is the Virtual Channel Identifier (VCI).
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays <b>N/A</b> when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays <b>N/A</b> when there is no VLAN ID number assigned.
ATM QoS	This shows the ATM Quality of Service (QoS) type configured for this connection. This displays <b>N/A</b> when there is no ATM QoS assigned.
IGMP Proxy	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
NAT	This shows whether NAT is activated or not for this connection. NAT is not available when the connection uses the bridging service.



**Table 6** Network Setting > Broadband (continued)

LABEL	DESCRIPTION
Default Gateway	This shows whether the Device uses the interface of this connection as the system default gateway.
Modify	Click the <b>Edit</b> icon to configure the connection.  Click the <b>Delete</b> icon to delete this connection from the Device. A window displays asking you to confirm that you want to delete the connection.

## 5.2.1 Add/Edit Internet Connection

Use this screen to configure a WAN connection. The screen varies depending on the interface type, encapsulation, and WAN service type you select.

### 5.2.1.1 Routing- PPPoE (VDSL/EtherWAN)

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **VDSL** or **EtherWAN** as the interface type, **Routing** as the encapsulation mode, and **PPPoE** as the WAN service type.

**Figure 17** Broadband Add/Edit: Routing- PPPoE (VDSL/EtherWAN)

**General**

Name :

Type :

Mode :

WANSericeType :

IPv6/IPv4 DualStack :

**VLAN**

Enable VLAN : ☐

Enter 802.1P Priority [0-7] :

Enter 802.1Q VLAN ID [1-4094] :  (3900 ~ 3905 are reserved.)

**PPP Information**

PPPUserName :

PPPPassword :

PPPoEServiceName :

Authentication Method :

Use Static IP Address : ☒

IP Address :

**Routing Feature**

NAT Enable : ☐

IGMP Proxy Enable : ☐

Apply as Default Gateway : ☐

**DNS Server**

☐ Obtain DNS info Automatically

☒ Use the following Static DNS IP Address

Primary DNS Server :

Secondary DNS Server :

**IPv6 Address**

☐ Obtain IPv6 Address Automatically

Enable Prefix Delegation : ☐

☒ Static IPv6 Address

IPv6 Address :

Prefix length :

IPv6 Default Gateway :

☐ 6to4 Tunneling

**IPv6 DNS Server**

☐ Obtain IPv6 DNS info Automatically

☒ Use the following Static DNS IPv6 Address

Primary IPv6 DNS Server :

Secondary IPv6 DNS Server :

**Figure 18** 6to4 Tunneling

☒ 6to4 Tunneling

6RD Enable : ☐

6to4 Tunneling Relay Server IP :

The following table describes the fields in this screen. /EtherWAN

**Table 7** Broadband Add/Edit: Routing- PPPoE (VDSL)

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	<p>Select <b>VDSL</b> or <b>EtherWAN</b> as the interface that you want to configure.</p> <p><b>VDSL</b>: The Device uses the VDSL technology for data transmission over the DSL port.</p> <p><b>EtherWAN</b>: The Device transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.</p>
Mode	Select <b>Routing</b> (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.
WAN Service Type	<p>This field is available only when you select <b>Routing</b> in the <b>Mode</b> field. Select the method of encapsulation used by your ISP.</p> <ul style="list-style-type: none"> <li>• <b>PPP over Ethernet (PPPoE)</b> - PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access.</li> <li>• <b>IP over Ethernet</b> - In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment.</li> </ul>
IPv6/IPv4 DualStack	Select <b>Enable</b> to allow the Device to run IPv4 and IPv6 at the same time. If this function is disabled, the Device only runs IPv4.
VLAN	This section is available only when you select <b>VDSL</b> or <b>EtherWAN</b> in the <b>Type</b> field.
Enable VLAN	Select this to add the VLAN tag (specified below) to the outgoing traffic through this connection.
Enter 802.1P Priority	<p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.</p> <p>Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.</p>
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
PPP Information	This section is available only when you select <b>Routing</b> in the <b>Mode</b> field and <b>PPPoE</b> in the <b>WAN Service Type</b> field.
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here.
Authentication Mode	<p>The Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.</p> <p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <ul style="list-style-type: none"> <li>• <b>AUTO</b>: Your Device accepts either CHAP or PAP when requested by this remote node.</li> <li>• <b>CHAP</b>: Your Device accepts CHAP only.</li> <li>• <b>PAP</b>: Your Device accepts PAP only.</li> <li>• <b>MS-CHAP</b>: Your Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.</li> </ul>

**Table 7** Broadband Add/Edit: Routing- PPPoE (VDSL) (continued)

LABEL	DESCRIPTION
Use Static IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you want to get a dynamic IP address from the ISP.
IP Address	Enter the static IP address provided by your ISP.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.  Select this option to have the Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the Device use the WAN interface of this connection as the system default gateway.
DNS Server	The section is not available when you select <b>Bridge</b> in the <b>WAN Service Type</b> field.
Obtain DNS info Automatically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
IPv6 Address	This section is not available when you select <b>Disable</b> in the <b>IPv6/IPv4 DualStack</b> field.
Obtain IPv6 Address Automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Enable Prefix Delegation	Select this to enable Prefix Delegation. This enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN.
Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the static IPv6 address provided by your ISP using colon (:) hexadecimal notation.
Prefix length	Enter the bit number of the IPv6 subnet mask provided by your ISP.
IPv6 Default Gateway	Enter the IPv6 address of the default outgoing gateway using a colon (:) hexadecimal notation.
6to4 Tunneling	Select 6to4 if the Device is connected to a network that has both IPv6 and IPv4 and the IPv4 addresses are public IP addresses. In this mode, the Device can convert an IPv4 address directly to an IPv6 address. The format is:  2002:[IPv4 address in hexadecimal]::/48  If you select this option, the fields shown in <a href="#">Figure 18</a> appear.

**Table 7** Broadband Add/Edit: Routing- PPPoE (VDSL) (continued)

LABEL	DESCRIPTION
6RD Enable	<p>Select this option to enable IPv6 Rapid Deployment. By enabling this function, the Device uses an ISP's IPv6 address prefix instead of the 2002::/48 prefix. The operational domain of 6RD is limited to and controlled by the ISP's network. 6RD hosts are ensured to be reachable from all native IPv6 addresses as 6RD only uses relay servers within control of the ISP.</p> <p>This option is not available if your <b>WAN Service Type</b> is <b>PPPoE</b>.</p>
6to4 Tunneling Relay Server IP	<p>Enter the tunneling relay server's IPv4 address in this field. If your <b>WAN Service Type</b> is <b>PPPoE</b>, you need to enter this field in order to use 6to4 Tunneling.</p>
IPv6 DNS Server	<p>Select whether you want to obtain the IPv6 DNS server addresses automatically or configure them manually.</p>
Obtain IPv6 DNS info Automatically	<p>Select this to have the Device get the IPv6 DNS server addresses from the ISP automatically.</p>
Use the following Static DNS IPv6 Address	<p>Select this to have the Device use the DNS server addresses you configure manually.</p>
Primary IPv6 DNS Server	<p>Enter the first IPv6 DNS server address assigned by the ISP.</p>
Secondary IPv6 DNS Server	<p>Enter the second IPv6 DNS server address assigned by the ISP.</p>
Apply	<p>Click <b>Apply</b> to save your changes.</p>
Back	<p>Click <b>Back</b> to return to the previous screen.</p>

### 5.2.1.2 Routing- IPoE (VDSL)

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **VDSL** or **EtherWAN** as the interface type, **Routing** as the encapsulation mode and **IP over Ethernet** as the WAN service type.

**Figure 19** Broadband Add/Edit: Routing- IPoE (VDSL/EtherWAN)

**Figure 20** 6to4 Tunneling

The following table describes the fields in this screen.

**Table 8** Broadband Add/Edit: Routing- IPoE (VDSL/EtherWAN)

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	Select <b>VDSL</b> or <b>EtherWAN</b> as the interface that you want to configure.  <b>VDSL:</b> The Device uses the VDSL technology for data transmission over the DSL port.  <b>EtherWAN:</b> The Device transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.
Mode	Select <b>Routing</b> (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.

**Table 8** Broadband Add/Edit: Routing- IPoE (VDSL/EtherWAN) (continued)

LABEL	DESCRIPTION
WAN Service Type	<p>This field is available only when you select <b>Routing</b> in the <b>Mode</b> field. Select the method of encapsulation used by your ISP.</p> <ul style="list-style-type: none"> <li>• <b>PPP over Ethernet (PPPoE)</b> - PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access.</li> <li>• <b>IP over Ethernet</b> - In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment.</li> </ul>
IPv6/IPv4 DualStack	Select <b>Enable</b> to allow the Device to run IPv4 and IPv6 at the same time. If this function is disabled, the Device only runs IPv4.
VLAN	This section is available only when you select <b>VDSL</b> or <b>EtherWAN</b> in the <b>Type</b> field.
Enable VLAN	Select this to add the VLAN tag (specified below) to the outgoing traffic through this connection.
Enter 802.1P Priority	<p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.</p> <p>Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.</p>
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
IP Address	This section is available only when you select <b>Routing</b> in the <b>Mode</b> field and <b>IPoE</b> in the <b>WAN Service Type</b> field.
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the Device in DHCP requests that the Device sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	<p>Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p> <p>Select this option to have the Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.</p>
Apply as Default Gateway	Select this option to have the Device use the WAN interface of this connection as the system default gateway.
DNS Server	This is available only when you select <b>Apply as Default Gateway</b> in the <b>Routing Feature</b> field.
Obtain DNS info Automatically	Select this to have the Device get the DNS server addresses from the ISP automatically.

**Table 8** Broadband Add/Edit: Routing- IPoE (VDSL/EtherWAN) (continued)

LABEL	DESCRIPTION
Use the following Static DNS IP Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
IPv6 Address	This section is not available when you select <b>Disable</b> in the <b>IPv6/IPv4 DualStack</b> field.
Obtain IPv6 Address Automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Enable Prefix Delegation	Select this to enable Prefix Delegation. This enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN.
Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the static IPv6 address provided by your ISP using colon (:) hexadecimal notation.
Prefix length	Enter the bit number of the IPv6 subnet mask provided by your ISP.
IPv6 Default Gateway	Enter the IPv6 address of the default outgoing gateway using a colon (:) hexadecimal notation.
6to4 Tunneling	Select 6to4 if the Device is connected to a network that has both IPv6 and IPv4 and the IPv4 addresses are public IP addresses. In this mode, the Device can convert an IPv4 address directly to an IPv6 address. The format is:  2002:[IPv4 address in hexadecimal]::/48  If you select this option, the fields shown in <a href="#">Figure 20</a> appear.
6RD Enable	Select this option to enable IPv6 Rapid Deployment. By enabling this function, the Device uses an ISP's IPv6 address prefix instead of the 2002::/48 prefix. The operational domain of 6RD is limited to and controlled by the ISP's network. 6RD hosts are ensured to be reachable from all native IPv6 addresses as 6RD only uses relay servers within control of the ISP.  This option is not available if your <b>WAN Service Type</b> is <b>PPPoE</b> .
6to4 Tunneling Relay Server IP	Enter the tunneling relay server's IPv4 address in this field. If your <b>WAN Service Type</b> is <b>PPPoE</b> , you need to enter this field in order to use 6to4 Tunneling.
IPv6 DNS Server	Select whether you want to obtain the IPv6 DNS server addresses automatically or configure them manually.
Obtain IPv6 DNS info Automatically	Select this to have the Device get the IPv6 DNS server addresses from the ISP automatically.
Use the following Static DNS IPv6 Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary IPv6 DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen.

### 5.2.1.3 Routing- PPPoE (ADSL)

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **ADSL** as the interface type, **Routing** as the encapsulation mode, and **PPPoE** as the WAN service type.

**Figure 21** Broadband Add/Edit: Routing- PPPoE (ADSL)

**General**

Name :

Type : 

ADSL

Mode : 

Routing

WANSerivceType : 

PPP over Ethernet(PPPoE)

PPPoE Passthrough ☐

IPv6/IPv4 DualStack : 

Enable

**ATM PVC Configuration**

VPI [0-255] :

VCI [32-65535] :

DSL Link Type : 

EoA

Encapsulation Mode : 

LLC/SNAP-BRIDGING

Service Category : 

Non Realtime VBR

Peak Cell Rate[cells/s] :

Sustainable Cell Rate[cells/s] :

Maximum Burst Size [cells] :

**PPP Infomation**

PPPUserName :

PPPPassword :

PPPoEServiceName :

Authentication Method : 

Auto

Use Static IP Address ☒

IP Address :

**Routing Feature**

NAT Enable : ☐

IGMP Proxy Enable : ☐

Apply as Default Gateway : ☐

**DNS Server**

☐ Obtain DNS info Automatically

☒ Use the following Static DNS IP Address

Primary DNS Server :

Secondary DNS Server :

**IPv6 Address**

☐ Obtain IPv6 Address Automatically

Enable Prefix Delegation ☐

☒ Static IPv6 Address

IPv6 Address :

Prefix length : 

64

IPv6 Default Gateway :

☐ 6to4 Tunneling

**IPv6 DNS Server**

☐ Obtain IPv6 DNS info Automatically

☒ Use the following Static DNS IPv6 Address

Primary IPv6 DNS Server :

Secondary IPv6 DNS Server :

Apply

Back

**Figure 22** 6to4 Tunneling

☒ 6to4 Tunneling

6RD Enable ☐

6to4 Tunneling Relay Server IP:

The following table describes the fields in this screen.

**Table 9** Broadband Add/Edit: Routing- PPPoE (ADSL)

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	Select <b>ADSL</b> as the interface that you want to configure. The Device uses the ADSL technology for data transmission over the DSL port.
Mode	Select <b>Routing</b> (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.



**Table 9** Broadband Add/Edit: Routing- PPPoE (ADSL) (continued)

LABEL	DESCRIPTION
WAN Service Type	<p>This field is available only when you select <b>Routing</b> in the <b>Mode</b> field. Select <b>PPPoE</b> as the method of encapsulation used by your ISP.</p> <ul style="list-style-type: none"> <li>• <b>PPP over Ethernet (PPPoE)</b> - PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access.</li> </ul>
IPv6/IPv4 DualStack	<p>Select <b>Enable</b> to allow the Device to run IPv4 and IPv6 at the same time. If this function is disabled, the Device only runs IPv4.</p>
ATM PVC Configuration	<p>VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.</p> <p>This section is available only when you select <b>ADSL</b> in the <b>Type</b> field to configure an ATM layer-2 interface.</p>
VPI	<p>The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.</p>
VCI	<p>The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.</p>
DSL Link Type	<p>The DSL link type is set to <b>EoA</b> (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. <b>EoA</b> supports IPoE, PPPoE and RFC1483/2684 bridging encapsulation methods.</p>
Encapsulation Mode	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are:</p> <ul style="list-style-type: none"> <li>• <b>LLC/SNAP-BRIDGING:</b> In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when the <b>DSL Link Type</b> is set to <b>EoA</b>.</li> <li>• <b>VC/MUX:</b> In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.</li> </ul>
Service Category	<p>Select <b>UBR Without PCR</b> for applications that are non-time sensitive, such as e-mail.</p> <p>Select <b>CBR</b> (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select <b>Non Realtime VBR</b> (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select <b>Realtime VBR</b> (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
Peak Cell Rate	<p>Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.</p> <p>This field is not available when you select <b>UBR Without PCR</b>.</p>
Sustainable Cell Rate	<p>The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.</p> <p>This field is available only when you select <b>Non Realtime VBR</b> or <b>Realtime VBR</b>.</p>

**Table 9** Broadband Add/Edit: Routing- PPPoE (ADSL) (continued)

LABEL	DESCRIPTION
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.  This field is available only when you select <b>Non Realtime VBR</b> or <b>Realtime VBR</b> .
PPP Information	This section is available only when you select <b>Routing</b> in the <b>Mode</b> field and <b>PPPoE</b> or <b>PPPoA</b> in the <b>WAN Service Type</b> field.
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here.
Authentication Mode	The Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.  Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: <ul style="list-style-type: none"> <li>• <b>AUTO</b>: Your Device accepts either CHAP or PAP when requested by this remote node.</li> <li>• <b>CHAP</b>: Your Device accepts CHAP only.</li> <li>• <b>PAP</b>: Your Device accepts PAP only.</li> <li>• <b>MS-CHAP</b>: Your Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.</li> </ul>
Use Static IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you want to get a dynamic IP address from the ISP.
IP Address	Enter the static IP address provided by your ISP.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.  Select this option to have the Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the Device use the WAN interface of this connection as the system default gateway.
DNS Server	The section is not available when you select <b>Bridge</b> in the <b>WAN Service Type</b> field.
Obtain DNS info Automatically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
IPv6 Address	This section is not available when you select <b>Disable</b> in the <b>IPv6/IPv4 DualStack</b> field.

**Table 9** Broadband Add/Edit: Routing- PPPoE (ADSL) (continued)

LABEL	DESCRIPTION
Obtain IPv6 Address Automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Enable Prefix Delegation	Select this to enable Prefix Delegation. This enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN.
Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the static IPv6 address provided by your ISP using colon (:) hexadecimal notation.
Prefix length	Enter the bit number of the IPv6 subnet mask provided by your ISP.
IPv6 Default Gateway	Enter the IPv6 address of the default outgoing gateway using a colon (:) hexadecimal notation.
6to4 Tunneling	<p>Select 6to4 if the Device is connected to a network that has both IPv6 and IPv4 and the IPv4 addresses are public IP addresses. In this mode, the Device can convert an IPv4 address directly to an IPv6 address. The format is:</p> <p>2002:[IPv4 address in hexadecimal]::/48</p> <p>If you select this option, the fields shown in <a href="#">Figure 22</a> appear.</p>
6RD Enable	<p>Select this option to enable IPv6 Rapid Deployment. By enabling this function, the Device uses an ISP's IPv6 address prefix instead of the 2002::/48 prefix. The operational domain of 6RD is limited to and controlled by the ISP's network. 6RD hosts are ensured to be reachable from all native IPv6 addresses as 6RD only uses relay servers within control of the ISP.</p> <p>This option is not available if your <b>WAN Service Type</b> is <b>PPPoE</b> or <b>PPPoA</b>.</p>
6to4 Tunneling Relay Server IP	Enter the tunneling relay server's IPv4 address in this field. If your <b>WAN Service Type</b> is <b>PPPoE</b> or <b>PPPoA</b> , you need to enter this field in order to use 6to4 Tunneling.
IPv6 DNS Server	Select whether you want to obtain the IPv6 DNS server addresses automatically or configure them manually.
Obtain IPv6 DNS info Automatically	Select this to have the Device get the IPv6 DNS server addresses from the ISP automatically.
Use the following Static DNS IPv6 Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary IPv6 DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen.

5.2.1.4 Routing- PPPoA

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **ADSL** as the interface type, **Routing** as the encapsulation mode and **PPPoA** as the WAN service type.

Figure 23 Broadband Add/Edit: Routing- PPPoA (ADSL)

**General**

Name :

Type : 

ADSL

Mode : 

Routing

WANServiceType : 

PPP over ATM(PPPoA)

IPv6/IPv4 DualStack : 

Enable

**ATM PVC Configuration**

VPI [0-255] :

VCI [32-65535] :

DSL Link Type : 

PPPoA

Encapsulation Mode : 

LLC/SNAP-BRIDGING

Service Category : 

Non Realtime VBR

Peak Cell Rate[cells/s] :

Sustainable Cell Rate[cells/s] :

Maximum Burst Size [cells] :

**PPP Information**

PPPOUserName :

PPPOPassword :

Authentication Method : 

Auto

Use Static IP Address : ☒

IP Address :

**Routing Feature**

NAT Enable : ☐

IGMP Proxy Enable : ☐

Apply as Default Gateway : ☐

**DNS Server**

☐ Obtain DNS info Automatically

☒ Use the following Static DNS IP Address

Primary DNS Server :

Secondary DNS Server :

**IPv6 Address**

☐ Obtain IPv6 Address Automatically

☒ Static IPv6 Address

Enable Prefix Delegation : ☐

IPv6 Address :

Prefix length : 

64

IPv6 Default Gateway :

☐ 6to4 Tunneling

**IPv6 DNS Server**

☐ Obtain IPv6 DNS info Automatically

☒ Use the following Static DNS IPv6 Address

Primary IPv6 DNS Server :

Secondary IPv6 DNS Server :

Apply

Back

Figure 24 6to4 Tunneling

☒ 6to4 Tunneling

6to4 Tunneling

6RD Enable ☐

6to4 Tunneling Relay Server IP:

The following table describes the fields in this screen.

Table 10 Broadband Add/Edit: Routing- PPPoA (ADSL)

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	Select an interface for which you want to configure here.  <b>ADSL:</b> The Device uses the ADSL technology for data transmission over the DSL port.  <b>EtherWAN:</b> The Device transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.
Mode	Select <b>Routing</b> (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.

**Table 10** Broadband Add/Edit: Routing- PPPoA (ADSL) (continued)

LABEL	DESCRIPTION
WAN Service Type	<p>This field is available only when you select <b>Routing</b> in the <b>Mode</b> field. Select <b>PPPoA</b> as the method of encapsulation used by your ISP.</p> <ul style="list-style-type: none"> <li>• <b>PPP over ATM (PPPoA)</b> - PPPoA allows just one PPPoA connection over a PVC.</li> </ul>
IPv6/IPv4 DualStack	Select <b>Enable</b> to allow the Device to run IPv4 and IPv6 at the same time. If this function is disabled, the Device only runs IPv4.
ATM PVC Configuration	<p>VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.</p> <p>This section is available only when you select <b>ADSL</b> in the <b>Type</b> field to configure an ATM layer-2 interface.</p>
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	The DSL link type is set to <b>PPPoA</b> (PPP over ATM) to allow just one PPPoA connection over a PVC.
Encapsulation Mode	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are:</p> <p><b>LLC/SNAP-BRIDGING:</b> In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when the <b>DSL Link Type</b> is set to <b>EoA</b>.</p> <p><b>VC/MUX:</b> In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.</p>
Service Category	<p>Select <b>UBR Without PCR</b> for applications that are non-time sensitive, such as e-mail.</p> <p>Select <b>CBR</b> (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select <b>Non Realtime VBR</b> (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select <b>Realtime VBR</b> (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
Peak Cell Rate	<p>Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.</p> <p>This field is not available when you select <b>UBR Without PCR</b>.</p>
Sustainable Cell Rate	<p>The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.</p> <p>This field is available only when you select <b>Non Realtime VBR</b> or <b>Realtime VBR</b>.</p>
Maximum Burst Size	<p>Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.</p> <p>This field is available only when you select <b>Non Realtime VBR</b> or <b>Realtime VBR</b>.</p>
PPP Information	This section is available only when you select <b>Routing</b> in the <b>Mode</b> field and <b>PPPoE</b> or <b>PPPoA</b> in the <b>WAN Service Type</b> field.

**Table 10** Broadband Add/Edit: Routing- PPPoA (ADSL) (continued)

LABEL	DESCRIPTION
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
Authentication Mode	<p>The Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.</p> <p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p><b>AUTO:</b> Your Device accepts either CHAP or PAP when requested by this remote node.</p> <p><b>CHAP:</b> Your Device accepts CHAP only.</p> <p><b>PAP:</b> Your Device accepts PAP only.</p> <p><b>MS-CHAP:</b> Your Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.</p>
Use Static IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you want to get a dynamic IP address from the ISP.
IP Address	Enter the static IP address provided by your ISP.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	<p>Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p> <p>Select this option to have the Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.</p>
Apply as Default Gateway	Select this option to have the Device use the WAN interface of this connection as the system default gateway.
DNS Server	The section is not available when you select <b>Bridge</b> in the <b>WAN Service Type</b> field.
Obtain DNS info Automatically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
IPv6 Address	This section is not available when you select <b>Disable</b> in the <b>IPv6/IPv4 DualStack</b> field.
Obtain IPv6 Address Automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Enable Prefix Delegation	Select this to enable Prefix Delegation. This enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN.

**Table 10** Broadband Add/Edit: Routing- PPPoA (ADSL) (continued)

LABEL	DESCRIPTION
Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the static IPv6 address provided by your ISP using colon (:) hexadecimal notation.
Prefix length	Enter the bit number of the IPv6 subnet mask provided by your ISP.
IPv6 Default Gateway	Enter the IPv6 address of the default outgoing gateway using a colon (:) hexadecimal notation.
6to4 Tunneling	<p>Select 6to4 if the Device is connected to a network that has both IPv6 and IPv4 and the IPv4 addresses are public IP addresses. In this mode, the Device can convert an IPv4 address directly to an IPv6 address. The format is:</p> <p>2002:[IPv4 address in hexadecimal]::/48</p> <p>If you select this option, the fields shown in <a href="#">Figure 24</a> appear.</p>
6RD Enable	<p>Select this option to enable IPv6 Rapid Deployment. By enabling this function, the Device uses an ISP's IPv6 address prefix instead of the 2002::/48 prefix. The operational domain of 6RD is limited to and controlled by the ISP's network. 6RD hosts are ensured to be reachable from all native IPv6 addresses as 6RD only uses relay servers within control of the ISP.</p> <p>This option is not available if your <b>WAN Service Type</b> is <b>PPPoE</b> or <b>PPPoA</b>.</p>
6to4 Tunneling Relay Server IP	Enter the tunneling relay server's IPv4 address in this field. If your <b>WAN Service Type</b> is <b>PPPoE</b> or <b>PPPoA</b> , you need to enter this field in order to use 6to4 Tunneling.
IPv6 DNS Server	Select whether you want to obtain the IPv6 DNS server addresses automatically or configure them manually.
Obtain IPv6 DNS info Automatically	Select this to have the Device get the IPv6 DNS server addresses from the ISP automatically.
Use the following Static DNS IPv6 Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary IPv6 DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen.

5.2.1.5 Routing- IPoE (ADSL)

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **ADSL** as the interface type, **Routing** as the encapsulation mode and **IP over Ethernet** as the WAN service type.

Figure 25 Broadband Add/Edit: Routing- IPoE (ADSL)

General

Name :

Type :  
ADSL

Mode :  
Routing

WANServiceType :  
IP over Ethernet

IPv6/IPv4 DualStack :  
Enable

ATM PVC Configuration

VPI[0-255] :  
8

VCI[32-65535] :  
34

DSL Link Type :  
EoA

Encapsulation Mode :  
LLC/SNAP-BRIDGING

Service Category :  
Non Realtime VBR

Peak Cell Rate(cells/s) :

Sustainable Cell Rate(cells/s) :

Maximum Burst Size [cells] :

IP Address

☐ Obtain an IP Address Automatically

Enable DHCP Option 60 :  
☒

Vendor Class Identifier :

☒ Static IP Address

IP Address :  
0.0.0.0

SubnetMask :  
0.0.0.0

Gateway/IPAddress :  
0.0.0.0

Routing Feature

NAT Enable :  
☐

IGMP Proxy Enable :  
☐

Apply as Default Gateway :  
☐

DNS Server

☐ Obtain DNS info Automatically

☒ Use the following Static DNS IP Address

Primary DNS Server :

Secondary DNS Server :

IPv6 Address

☐ Obtain IPv6 Address Automatically

Enable Prefix Delegation  
☐

☒ Static IPv6 Address

IPv6 Address :

Prefix length :  
64

IPv6 Default Gateway :

☐ 6to4 Tunneling

IPv6 DNS Server

☐ Obtain IPv6 DNS info Automatically

☒ Use the following Static DNS IPv6 Address

Primary IPv6 DNS Server :

Secondary IPv6 DNS Server :

Apply

Back

Figure 26 6to4 Tunneling

☒ 6to4 Tunneling

6RD Enable  
☐

6to4 Tunneling Relay Server IP:  
192.88.22.33

The following table describes the fields in this screen.

Table 11 Broadband Add/Edit: Routing- IPoE (ADSL)

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	Select <b>ADSL</b> as the interface that you want to configure. The Device uses the ADSL technology for data transmission over the DSL port.
Mode	Select <b>Routing</b> (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.
WAN Service Type	<div>This field is available only when you select <b>Routing</b> in the <b>Mode</b> field. Select <b>IPoE</b> as the method of encapsulation used by your ISP.</div> <div><ul style="list-style-type: none"><li><b>IP over Ethernet</b> - In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment.</li></ul></div>



**Table 11** Broadband Add/Edit: Routing- IPoE (ADSL) (continued)

LABEL	DESCRIPTION
IPv6/IPv4 DualStack	Select <b>Enable</b> to allow the Device to run IPv4 and IPv6 at the same time. If this function is disabled, the Device only runs IPv4.
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.  This section is available only when you select <b>ADSL</b> in the <b>Type</b> field to configure an ATM layer-2 interface.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	The DSL link type is set to <b>EoA</b> (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. <b>EoA</b> supports IPoE, PPPoE and RFC1483/2684 bridging encapsulation methods.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list. Choices are:  <ul style="list-style-type: none"> <li>• <b>LLC/SNAP-BRIDGING:</b> In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when the <b>DSL Link Type</b> is set to <b>EoA</b>.</li> <li>• <b>VC/MUX:</b> In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.</li> </ul>
Service Category	Select <b>UBR Without PCR</b> for applications that are non-time sensitive, such as e-mail.  Select <b>CBR</b> (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.  Select <b>Non Realtime VBR</b> (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.  Select <b>Realtime VBR</b> (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.  This field is not available when you select <b>UBR Without PCR</b> .
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.  This field is available only when you select <b>Non Realtime VBR</b> or <b>Realtime VBR</b> .
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.  This field is available only when you select <b>Non Realtime VBR</b> or <b>Realtime VBR</b> .
IP Address	This section is available only when you select <b>Routing</b> in the <b>Mode</b> field and <b>IPoE</b> in the <b>WAN Service Type</b> field.

**Table 11** Broadband Add/Edit: Routing- IPoE (ADSL) (continued)

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the Device in DHCP requests that the Device sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.  Select this option to have the Device act as an IGMP proxy on this connection. This allows the Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the Device use the WAN interface of this connection as the system default gateway.
DNS Server	This is available only when you select <b>Apply as Default Gateway</b> in the <b>Routing Feature</b> field.
Obtain DNS info Automatically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
IPv6 Address	This section is not available when you select <b>Disable</b> in the <b>IPv6/IPv4 DualStack</b> field.
Obtain IPv6 Address Automatically	Select this option if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Enable Prefix Delegation	Select this to enable Prefix Delegation. This enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN.
Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the static IPv6 address provided by your ISP using colon (:) hexadecimal notation.
Prefix length	Enter the bit number of the IPv6 subnet mask provided by your ISP.
IPv6 Default Gateway	Enter the IPv6 address of the default outgoing gateway using a colon (:) hexadecimal notation.

**Table 11** Broadband Add/Edit: Routing- IPoE (ADSL) (continued)

LABEL	DESCRIPTION
6to4 Tunneling	Select 6to4 if the Device is connected to a network that has both IPv6 and IPv4 and the IPv4 addresses are public IP addresses. In this mode, the Device can convert an IPv4 address directly to an IPv6 address. The format is:  2002:[IPv4 address in hexadecimal]::/48  If you select this option, the fields shown in <a href="#">Figure 26</a> appear.
6RD Enable	Select this option to enable IPv6 Rapid Deployment. By enabling this function, the Device uses an ISP's IPv6 address prefix instead of the 2002::/48 prefix. The operational domain of 6RD is limited to and controlled by the ISP's network. 6RD hosts are ensured to be reachable from all native IPv6 addresses as 6RD only uses relay servers within control of the ISP.  This option is not available if your <b>WAN Service Type</b> is <b>PPPoE</b> or <b>PPPoA</b> .
6to4 Tunneling Relay Server IP	Enter the tunneling relay server's IPv4 address in this field. If your <b>WAN Service Type</b> is <b>PPPoE</b> or <b>PPPoA</b> , you need to enter this field in order to use 6to4 Tunneling.
IPv6 DNS Server	Select whether you want to obtain the IPv6 DNS server addresses automatically or configure them manually.
Obtain IPv6 DNS info Automatically	Select this to have the Device get the IPv6 DNS server addresses from the ISP automatically.
Use the following Static DNS IPv6 Address	Select this to have the Device use the DNS server addresses you configure manually.
Primary IPv6 DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen.

### 5.2.1.6 Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Bridge** as the encapsulation mode. The screen differs according to the interface type you select.

If you select **VDSL** or **EtherWAN** as the interface type, the following screen appears.

**Figure 27** Broadband Add/Edit: Bridge (VDSL/EtherWAN)

**General**

Name :

Type : **EtherWAN**

Mode : **Bridge**

**VLAN**

Enable VLAN : ☐

Enter 802.1P Priority [0-7] :

Enter 802.1Q VLAN ID [1-4094] :  (3900 ~ 3905 are reserved.)

**Bridge Group**

Select LAN/WLAN port(s) you wish to together with this WAN interface

Available LAN/WLAN Port(s)      Bridged LAN/WLAN Port(s)

LAN1      Add >>  
LAN2      Remove <<  
LAN3  
LAN4  
ZyXEL

**Apply** **Back**

The following table describes the fields in this screen.

**Table 12** Broadband Add/Edit: Bridge (VDSL/EtherWAN)

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	Select <b>VDSL</b> or <b>EtherWAN</b> as the interface that you want to configure.  <b>VDSL</b> : The Device uses the VDSL technology for data transmission over the DSL port.  <b>EtherWAN</b> : The Device transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.
Mode	Select <b>Bridge</b> when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select <b>Bridge</b> , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	This section is available only when you select <b>VDSL</b> or <b>EtherWAN</b> in the <b>Type</b> field.
Enable VLAN	Select this to add the VLAN Tag (specified below) to the outgoing traffic through this connection.
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.  Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.

**Table 12** Broadband Add/Edit: Bridge (VDSL/EtherWAN) (continued)

LABEL	DESCRIPTION
Bridge Group	<p>Select the LAN/WLAN port(s) from which traffic will be forwarded to the WAN interface directly.</p> <p>Select a port from the <b>Available LAN/WLAN Port(s)</b> list and click <b>Add &gt;&gt;</b> to add it to the <b>Bridged LAN/WLAN Port(s)</b> list.</p> <p>If you want to remove a port from the <b>Bridged LAN/WLAN Port(s)</b> list, select it and click <b>Remove &lt;&lt;</b>.</p> <p>You cannot configure a QoS class for traffic from the LAN port which is selected here.</p>
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen.

If you select **ADSL** as the interface type, the following screen appears.

**Figure 28** Broadband Add/Edit: Bridge (ADSL)

**General**

Name :

Type :

Mode :

**Bridge Group**

Select LAN/WLAN port(s) you wish to together with this WAN interface

Available LAN/WLAN Port(s)      Bridged LAN/WLAN Port(s)

LAN1    Add >>   

LAN2    Remove <<   

LAN3   

LAN4   

ZyXEL   

**ATM PVC Configuration**

VPI[0-255] :

VC[32-65535] :

Encapsulation Mode :

Service Category :

Peak Cell Rate[cells/s] :

Sustainable Cell Rate[cells/s] :

Maximum Burst Size [cells] :

Apply    Back

The following table describes the fields in this screen.

**Table 13** Broadband Add/Edit: Bridge (ADSL)

LABEL	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	Select <b>ADSL</b> as the interface for which you want to configure here. The Device uses the ADSL technology for data transmission over the DSL port.

**Table 13** Broadband Add/Edit: Bridge (ADSL) (continued)

LABEL	DESCRIPTION
Mode	Select <b>Bridge</b> when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select <b>Bridge</b> , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
Bridge Group	<p>Select the LAN/WLAN port(s) from which traffic will be forwarded to the WAN interface directly.</p> <p>Select a port from the <b>Available LAN/WLAN Port(s)</b> list and click <b>Add &gt;&gt;</b> to add it to the <b>Bridged LAN/WLAN Port(s)</b> list.</p> <p>If you want to remove a port from the <b>Bridged LAN/WLAN Port(s)</b> list, select it and click <b>Remove &lt;&lt;</b>.</p> <p>You cannot configure a QoS class for traffic from the LAN port which is selected here.</p>
ATM PVC Configuration	<p>VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.</p> <p>This section is available only when you select <b>ADSL</b> in the <b>Type</b> field to configure an ATM layer-2 interface.</p>
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Encapsulation Mode	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are:</p> <ul style="list-style-type: none"> <li>• <b>LLC/SNAP-BRIDGING:</b> In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header.</li> <li>• <b>VC/MUX:</b> In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.</li> </ul>
Service Category	<p>Select <b>UBR Without PCR</b> for applications that are non-time sensitive, such as e-mail.</p> <p>Select <b>CBR</b> (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select <b>Non Realtime VBR</b> (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select <b>Realtime VBR</b> (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
Peak Cell Rate	<p>Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.</p> <p>This field is not available when you select <b>UBR Without PCR</b>.</p>
Sustainable Cell Rate	<p>The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.</p> <p>This field is available only when you select <b>Non Realtime VBR</b> or <b>Realtime VBR</b>.</p>

**Table 13** Broadband Add/Edit: Bridge (ADSL) (continued)

LABEL	DESCRIPTION
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.  This field is available only when you select <b>Non Realtime VBR</b> or <b>Realtime VBR</b> .
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen.

## 5.3 The 3G Backup Screen

Use this screen to configure your 3G settings. Click **Broadband > 3G Backup**.

At the time of writing, the 3G card you can use in the Device is Huawei E220, E270, E160, E169G.

Note: The actual data rate you obtain varies depending the 3G card you use, the signal strength to the service provider's base station, and so on.

If the signal strength of a 3G network is too low, the 3G card may switch to an available 2.5G or 2.75G network. Refer to [Section 5.4 on page 117](#) for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

**Figure 29** Broadband > 3G Backup

3G Backup

☐ Enable 3G Backup

Card Description : N/A

Username :  (Optional)

Password :  (Optional)

PIN :  (Optional) Only for unlock PIN next time  
(PIN remaining authentication times: N/A)

Dial String :

APN :

Connection :

☒ Obtain an IP Address Automatically

☐ Use the following static IP address

☒ Obtain DNS info dynamically

☐ Use the following static DNS IP address

Primary DNS Server :

Secondary DNS Server :

The following table describes the labels in this screen.

**Table 14** Broadband > 3G Backup

LABEL	DESCRIPTION
3G Backup	Select <b>Enable 3G Backup</b> to have the Device use the 3G connection as your WAN or a backup when the wired WAN connection fails.
Card Description	This field displays the manufacturer and model name of your 3G card if you inserted one in the Device. Otherwise, it displays <b>N/A</b> .
Username	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
PIN	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card.  If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet.  If your ISP disabled PIN code authentication, leave this field blank.
Dial String	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number.  For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan.
APN Code	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method.  You can enter up to 32 ASCII printable characters. Spaces are allowed.
Connection	Select <b>Nailed-UP</b> if you do not want the connection to time out.  Select <b>On-Demand</b> if you do not want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the Device automatically disconnects from the ISP.
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected <b>Use the following static IP address</b> .
Obtain DNS info dynamically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the Device use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Apply	Click <b>Apply</b> to save your changes back to the Device.
Cancel	Click <b>Cancel</b> to return to the previous configuration.



## 5.4 Technical Reference

The following section contains additional technical information about the Device features described in this chapter.

### Encapsulation

Be sure to use the encapsulation method required by your ISP. The Device can work in bridge mode or routing mode. When the Device is in routing mode, it supports the following methods.

### IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

### PPP over ATM (PPPoA)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

### PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

### RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a

separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

## Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

### VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

### LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

## Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

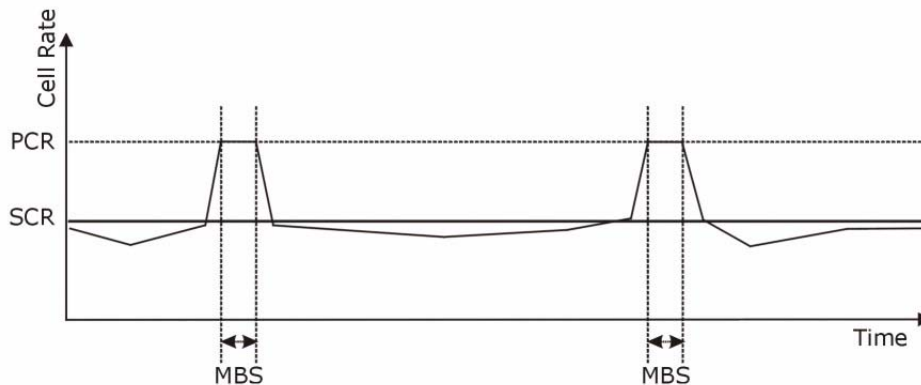
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

**Figure 30** Example of Traffic Shaping



## ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

### Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

### Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

### Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

## IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

## Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

## Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

## Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the Device queries all directly connected networks to gather group membership. After that, the Device periodically updates this information.

## DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of `www.zyxel.com` is `204.217.0.2`. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Device can get the DNS server addresses in the following ways.

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

## IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

## IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address

compose the network address. The prefix length is written as "/x" where x is a number. For example,


2001:db8:1a2b:15::1a2f:0/32

means that the first 32 bits (2001:db8) is the subnet prefix.

### 3G Comparison Table

See the following table for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

**Table 15** 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies

NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.	CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU <sup>A</sup> specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		
				Fast

A. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

# Wireless

## 6.1 Overview

This chapter describes the Device's **Network Setting > Wireless** screens. Use these screens to set up your Device's wireless connection.

### 6.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode ([Section 6.2 on page 125](#)).
- Use the **More AP** screen to set up multiple wireless networks on your Device ([Section 6.3 on page 131](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 6.4 on page 133](#)).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications ([Section 6.5 on page 135](#)).
- Use the **Scheduling** screen to schedule a time period for the wireless LAN to operate each day ([Section 6.6 on page 137](#)).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

### 6.1.2 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

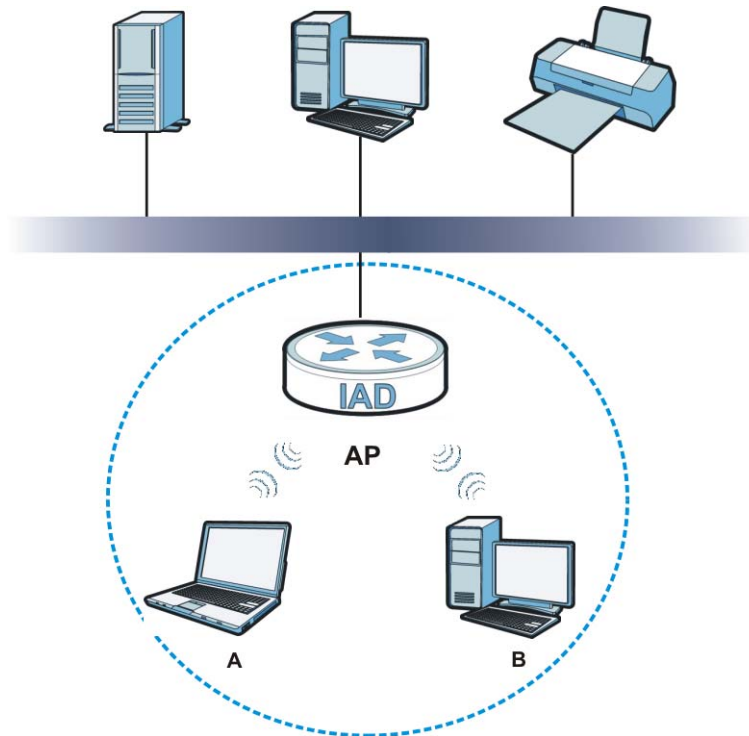
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

**Figure 31** Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.  
The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.  
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
- Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.



### 6.1.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See [Section 6.7 on page 137](#) if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.

- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

## 6.2 The Wireless General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the Device from a computer connected to the wireless LAN and you change the Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Device's new settings.

Click **Network Setting > Wireless** to open the **General** screen. Select the **Enable Wireless LAN** checkbox to show the Wireless configurations.

**Figure 32** Network Setting > Wireless > General

The screenshot displays the 'Wireless Network Setup' screen. At the top, under 'Wireless Network Settings', the 'Enable Wireless LAN' checkbox is checked. Below this, the 'Wireless Network Name(SSID)' is set to 'ZyXEL\_668C'. The 'BSSID' is '02:13:49:11:66:8c'. The 'Mode Select' dropdown is set to '802.11b/g/n', and the 'Channel Selection' dropdown is set to 'Channel 11'. The 'Operating Channel' is '11'. A 'Scan' button is located next to the channel selection. At the bottom, there is a 'Security Level' slider with three positions: 'No Security', 'Basic', and 'More Secure (Recommended)'. The slider is currently positioned at 'No Security'. 'Apply' and 'Cancel' buttons are at the bottom right.

The following table describes the labels in this screen.

**Table 16** Network > Wireless LAN > General

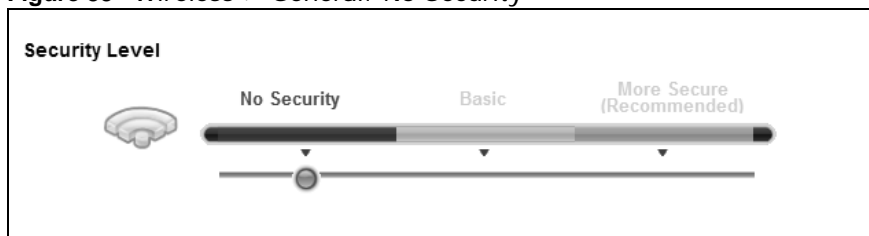
LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select the <b>Enable Wireless LAN</b> check box to activate the wireless LAN.
Wireless Network Settings	
Wireless Network Name (SSID)	<p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.</p> <p>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.</p>
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.
Mode Select	<p>This makes sure that only compliant WLAN devices can associate with the Device.</p> <p>Select <b>802.11b/g/n</b> to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Device. The transmission rate of your Device might be reduced.</p> <p>Select <b>802.11b/g</b> to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the Device. The transmission rate of your Device might be reduced.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the Device. Select <b>802.11n only in 2.4G band</b> to allow only IEEE 802.11n compliant WLAN devices with the same frequency range (2.4 GHz) to associate with the Device.</p>
Channel Selection	<p>Set the channel depending on your particular region.</p> <p>Select a channel or use <b>Auto</b> to have the Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the Device is currently using then displays in the <b>Operating Channel</b> field.</p>
Scan	Click this button to have the Device immediately scan for and select a channel (which is not used by another device) whenever the device reboots or the wireless setting is changed.
Operating Channel	This is the channel currently being used by your AP.
Security Level	
Security Mode	<p>Select <b>Basic</b> or <b>More Secure</b> to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. When you select to use a security, additional options appears in this screen.</p> <p>Or you can select <b>No Security</b> to allow any client to associate this network without any data encryption or authentication.</p> <p>See the following sections for more details about wireless security modes.</p>
Apply	Click <b>Apply</b> to save your changes back to the Device.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 6.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your Device, your network is accessible to any wireless networking device that is within range.

**Figure 33** Wireless > General: No Security



The following table describes the labels in this screen.

**Table 17** Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose <b>No Security</b> from the sliding bar.

## 6.2.2 Basic (Static WEP/Shared WEP Encryption)

WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

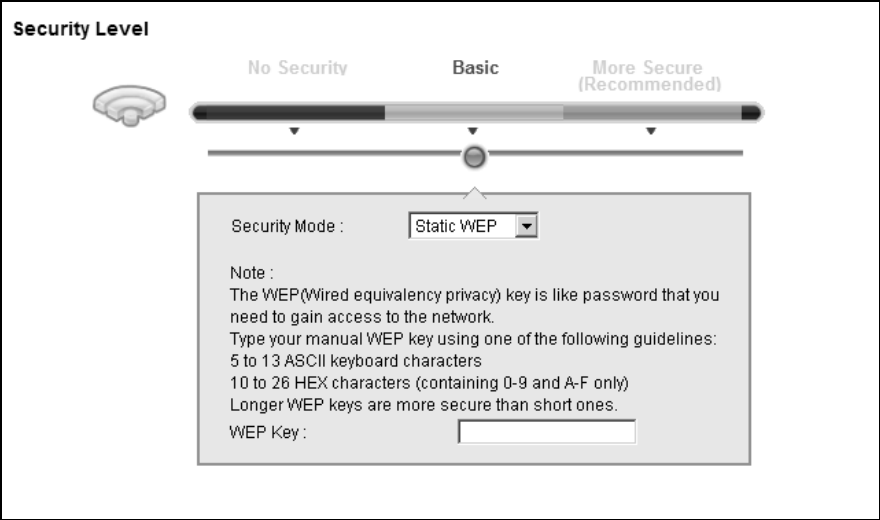
There are two types of WEP authentication namely, Open System (**Static WEP**) and Shared Key (**Shared WEP**).

Open system is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.

Shared key mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.

In order to configure and enable WEP encryption, click **Network Settings > Wireless** to display the **General** screen. Select **Basic** as the security level. Then select **Static WEP** or **Shared WEP** from the **Security Mode** list.

**Figure 34** Wireless > General: Basic (Static WEP/Shared WEP)



The following table describes the labels in this screen.

**Table 18** Wireless > General: Basic (Static WEP/Shared WEP)

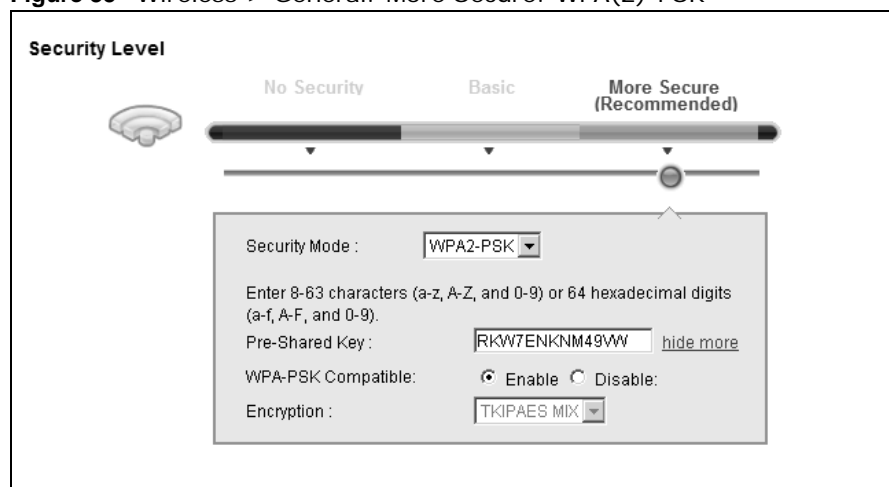
LABEL	DESCRIPTION
Security Mode	Choose <b>Static WEP</b> or <b>Shared WEP</b> from the drop-down list box. <ul style="list-style-type: none"><li>Select <b>Static WEP</b> to have the Device allow association with wireless clients that use Open System mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. The Device authenticates wireless clients using Shared Key mode that have the correct WEP key.</li><li>Select <b>Shared WEP</b> to have the Device authenticate only those wireless clients that use Shared Key mode and have the correct WEP key.</li></ul>
WEP Key	Enter a WEP key that will be used to encrypt data. Both the Device and the wireless stations must use the same WEP key for data transmission.  If you want to manually set the WEP key, enter any 5 or 13 characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively.

### 6.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Settings** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

**Figure 35** Wireless > General: More Secure: WPA(2)-PSK



The following table describes the labels in this screen.

**Table 19** Wireless > General: WPA(2)-PSK

LABEL	DESCRIPTION
Security Level	Select <b>More Secure</b> to enable WPA(2)-PSK data encryption.
Security Mode	Select <b>WPA-PSK</b> or <b>WPA2-PSK</b> from the drop-down list box.
Pre-Shared Key	The encryption mechanisms used for <b>WPA/WPA2</b> and <b>WPA-PSK/WPA2-PSK</b> are the same. The only difference between the two is that <b>WPA-PSK/WPA2-PSK</b> uses a simple common password, instead of user-specific credentials.  Type a pre-shared key from 8 to 63 case-sensitive ASCII characters or 64 hexadecimal digits.
more.../hide more	Click <b>more...</b> to show more fields in this section. Click <b>hide more</b> to hide them.

**Table 19** Wireless > General: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
WPA-PSK Compatible	This field appears when you choose <b>WPA-PSK2</b> as the <b>Security Mode</b> .  Check this field to allow wireless devices using <b>WPA-PSK</b> security mode to connect to your Device. The Device supports WPA-PSK and WPA2-PSK simultaneously.
Encryption	If the security mode is <b>WPA-PSK</b> , the encryption mode is set to <b>TKIP</b> to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network.  If the security mode is <b>WPA-PSK2</b> and <b>WPA-PSK Compatible</b> is disabled, the encryption mode is set to <b>AES</b> to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP.  If the security mode is <b>WPA-PSK2</b> and <b>WPA-PSK Compatible</b> is enabled, the encryption mode is set to <b>TKIPAES MIX</b> to allow both TKIP and AES types of security in your wireless network.

## 6.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

Click **Network Settings > Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA** or **WPA2** from the **Security Mode** list.

**Figure 36** Wireless > General: More Secure: WPA(2)

**Security Level**

No Security      Basic      **More Secure (Recommended)**

Security Mode : WPA2

Authentication Server

IP Address :

Port Number : 1812

Shared Secret :  [hide more](#)

WPA Compatible : ☐ Enable ☒ Disable

Group Key Update Timer: 0 sec

Encryption : AES

The following table describes the labels in this screen.

**Table 20** Wireless > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Level	Select <b>More Secure</b> to enable WPA(2)-PSK data encryption.
Security Mode	Choose <b>WPA</b> or <b>WPA2</b> from the drop-down list box.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is <b>1812</b> .  You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the Device.  The key must be the same on the external authentication server and your Device. The key is not sent over the network.
more.../hide more	Click <b>more...</b> to show more fields in this section. Click <b>hide more</b> to hide them.
WPA Compatible	This field is only available for WPA2. Select this if you want the Device to support WPA and WPA2 simultaneously.
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the RADIUS server sends a new group key out to all clients.  If the value is set to "0", the update timer function is disabled.
Encryption	If the security mode is <b>WPA</b> , the encryption mode is set to <b>TKIP</b> to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network.  If the security mode is <b>WPA2</b> , the encryption mode is set to <b>AES</b> to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP.







## 6.3 The More AP Screen

The Device can broadcast up to four wireless network names at the same time. This means that users can connect to the Device using different SSIDs. You can secure the connection on each SSID profile so that wireless clients connecting to the Device using different SSIDs cannot communicate with each other.

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the Device.

Click **Network Settings > Wireless > More AP**. The following screen displays.

**Figure 37** Network Settings > Wireless > More AP

#	Active	SSID	Security	Modify
2		ZyXEL_668D	WPA2-PSK mixed	
3		ZyXEL_668E	WPA2-PSK mixed	
4		ZyXEL_668F	WPA2-PSK mixed	

The following table describes the labels in this screen.

**Table 21** Network Settings > Wireless > More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Active	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.
SSID	<p>An SSID profile is the set of parameters relating to one of the Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated.</p> <p>This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.</p>
Security	This field indicates the security mode of the SSID profile.
Modify	Click the <b>Edit</b> icon to configure the SSID profile.

### 6.3.1 Edit More AP

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

**Figure 38** Wireless > More AP: Edit

**Wireless Network Setup**

Wireless : ☐ Enable Wireless LAN

**Wireless Network Settings**

Wireless Network Name/SSID: ZyXEL\_668D

☐ Hide SSID

BSSID : 02:13:49:11:66:8d

**Security Level**

No Security Basic **More Secure (Recommended)**

Security Mode : WPA2-PSK

Enter 8-63 characters (a-z, A-Z, and 0-9) or 64 hexadecimal digits (a-f, A-F, and 0-9).

Pre-Shared Key : 9JFY4TCVHF49J [more...](#)

Apply Back

The following table describes the fields in this screen.

**Table 22** Wireless > More AP: Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select the <b>Enable Wireless LAN</b> check box to activate the wireless LAN.
Wireless Network Settings	



**Table 22** Wireless > More AP: Edit (continued)

LABEL	DESCRIPTION
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.  Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.
Security Level	
Security Mode	Select <b>Basic (WEP)</b> or <b>More Secure (WPA(2)-PSK, WPA(2))</b> to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. After you select to use a security, additional options appears in this screen.  Or you can select <b>No Security</b> to allow any client to associate this network without any data encryption or authentication.  See <a href="#">Section 6.2.1 on page 127</a> for more details about this field.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to exit this screen without saving.

## 6.4 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See [Section 6.7.6.3 on page 144](#) for more information about WPS.

Note: The Device applies the security settings of the **SSID1** profile (see [Section 6.2 on page 125](#)). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network Setting > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.


**Figure 39** Network Setting > Wireless > WPS

General


WPS : ☒ Enable ☐ Disable

Add a new device with WPS Method

 **Method 1 PBC**

Step 1.Click WPS button 

Step 2.Press the WPS button on your new wireless client device within 120 seconds

 **Method 2 PIN**

Step 1. Enter the PIN of your new wireless client device and then click Register

Step 2.Press the WPS button on your new wireless client device within 120 seconds

WPS Configuration Summary

AP PIN : 11403647

Status : Not Configured

802.11 Mode :

SSID :

Security :

Note :

This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured.

The following table describes the labels in this screen.

**Table 23** Network Setting > Wireless > WPS

LABEL	DESCRIPTION
Enable WPS	Select <b>Enable</b> to activate WPS on the Device.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
WPS	<div>Click this button to add another WPS-enabled wireless device (within wireless range of the Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the <b>WPS</b> button on this screen.</div> <div>Note: You must press the other wireless device's WPS button within two minutes of pressing this button.</div>
Method 2 PIN	Use this section to set up a WPS wireless network by entering the PIN (Personal Identification Number) of the client into the Device.

**Table 23** Network Setting > Wireless > WPS (continued)

LABEL	DESCRIPTION
Register	<p>Enter the PIN of the device that you are setting up a WPS connection with and click <b>Register</b> to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Device.</p>
WPS Configuration Summary	
AP PIN	<p>The PIN of the Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS.</p> <p>The PIN is not necessary when you use WPS push-button method.</p> <p>Click the <b>Generate New PIN</b> button to have the Device create a new PIN.</p>
Status	<p>This displays <b>Configured</b> when the Device has connected to a wireless network using WPS or <b>Enable WPS</b> is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen.</p> <p>This displays <b>Not Configured</b> when there is no wireless or wireless security changes on the Device or you click <b>Release Configuration</b> to remove the configured wireless and wireless security settings.</p>
Release Configuration	<p>This button is available when the WPS status is <b>Configured</b>.</p> <p>Click this button to remove all configured wireless and wireless security settings for WPS connections on the Device.</p>
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the Device.
SSID	This is the name of the wireless network.
Security	This is the type of wireless security employed by the network.
Apply	Click <b>Apply</b> to save your changes.

## 6.5 The WMM Screen

Use this screen to enable or disable Wi-Fi MultiMedia (WMM) wireless networks for multimedia applications.

Click **Network Setting > Wireless > WMM**. The following screen displays.

**Figure 40** Network Setting > Wireless > WMM

**WMM (WiFi MultiMedia)**

☒ Enable WMM of SSID1

☒ Enable WMM of SSID2

☒ Enable WMM of SSID3

☒ Enable WMM of SSID4

☐ Enable WMM Automatic Power Save Delivery(APSD)

Apply

Cancel

The following table describes the labels in this screen.

**Table 24** Network Setting > Wireless > WMM

LABEL	DESCRIPTION
Enable WMM of SSID1~4	This enables the Device to automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Enable WMM Automatic Power Save Deliver (APSD)	Click this to increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 6.6 Scheduling Screen

Click **Network Setting > Wireless > Scheduling** to open the **Wireless LAN Scheduling** screen. Use this screen to configure when the Device enables or disables the wireless LAN.

**Figure 41** Network Setting > Wireless > Scheduling

Wireless LAN Scheduling : ☐ Enable ☒ Disable

WLAN Status	Day	Between the following times (24-Hour Format)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Everyday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Mon.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Tue.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Wed.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Thu.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Fri.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Sat.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Sun.	00 (hour) 00 (min) ~ 00 (hour) 00 (min)

**Note :**  
Specify the same begin time and end time means the whole day schedule.

**Apply** **Cancel**

The following table describes the labels in this screen.

**Table 25** Network Setting > Wireless > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	Select <b>Enable</b> to activate wireless LAN scheduling on your Device.
WLAN status	Select <b>On</b> or <b>Off</b> to enable or disable the wireless LAN.
Day	Select the day(s) you want to turn the wireless LAN on or off.
Between the following times	Specify the time period during which to apply the schedule. For example, you want the wireless network to be only available during work hours. Check Mon ~ Fri in the day column, and specify 8:00 ~ 18:00 in the time table.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 6.7 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

## 6.7.1 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the Device's web configurator.

**Table 26** Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the Device. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the Device.</p>
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the Device does, it cannot communicate with the Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

## 6.7.2 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

### 6.7.2.1 SSID

Normally, the Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

### 6.7.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.<sup>1</sup> A MAC address is usually written using twelve hexadecimal characters<sup>2</sup>; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

### 6.7.2.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.


- 
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
  2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

### 6.7.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See [Section 6.7.2.3 on page 139](#) for information about this.)

**Table 27** Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest 	No Security	WPA
	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

**Note:** It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

### 6.7.3 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

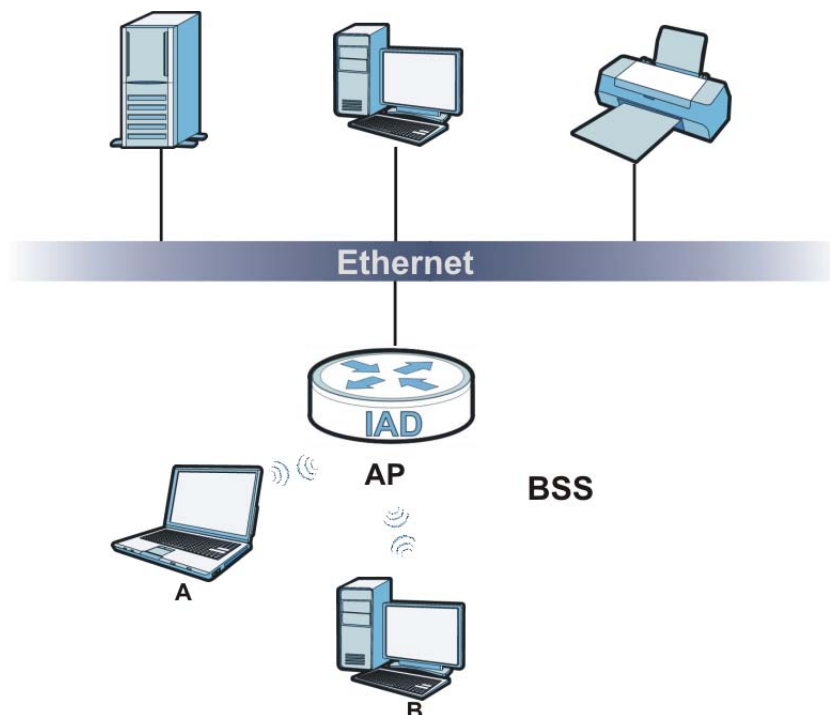


## 6.7.4 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

**Figure 42** Basic Service set



## 6.7.5 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

### 6.7.5.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

## 6.7.6 WiFi Protected Setup (WPS)

Your Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

### 6.7.6.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Device, see [Section 6.4 on page 133](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the Device you must press the WPS button for more than three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

### 6.7.6.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated

on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

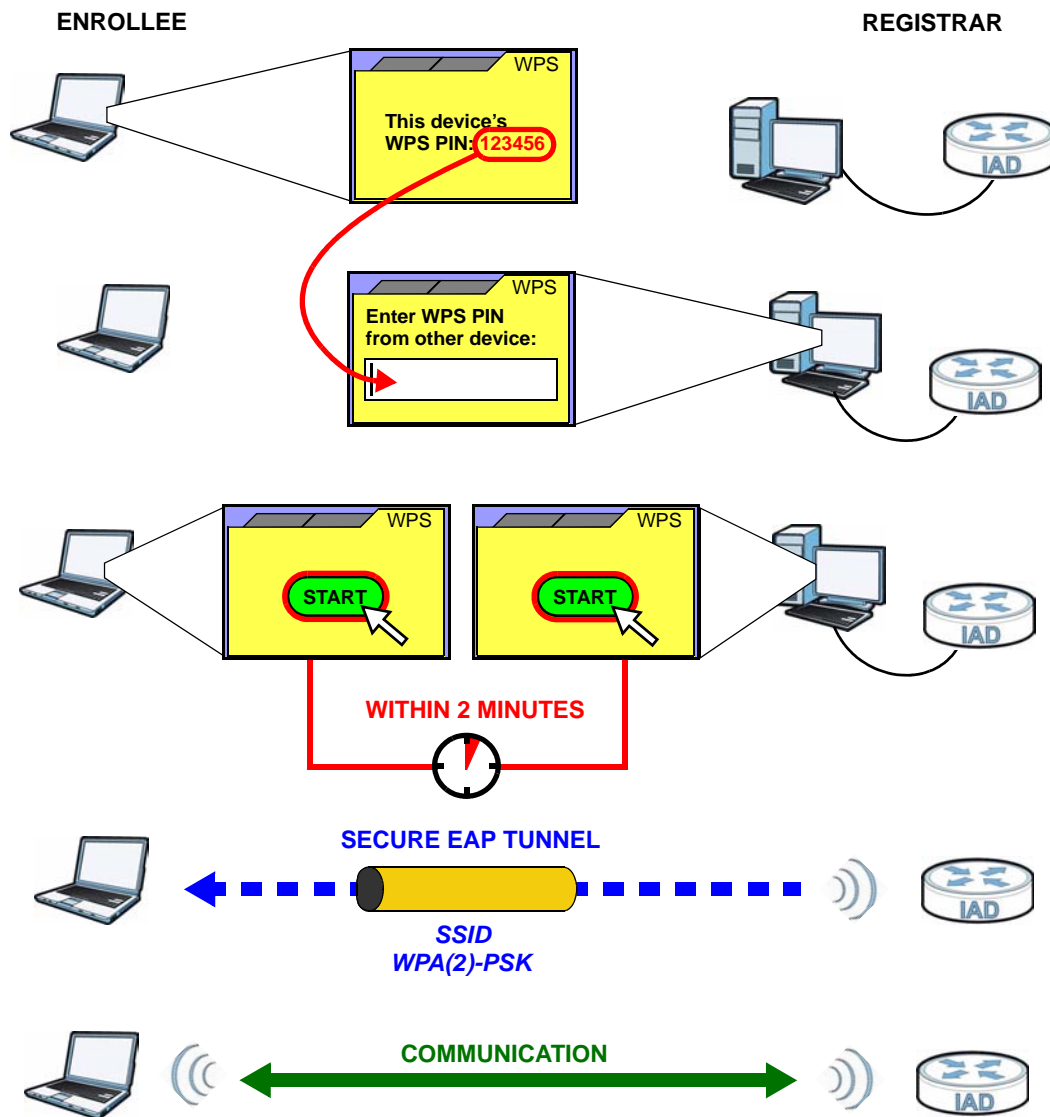
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1** Ensure WPS is enabled on both devices.
- 2** Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3** Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the Device, see [Section 6.4 on page 133](#)).
- 4** Enter the client's PIN in the AP's configuration interface.
- 5** If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6** Start WPS on both devices within two minutes.
- 7** Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8** On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

**Figure 43** Example WPS Process: PIN Method

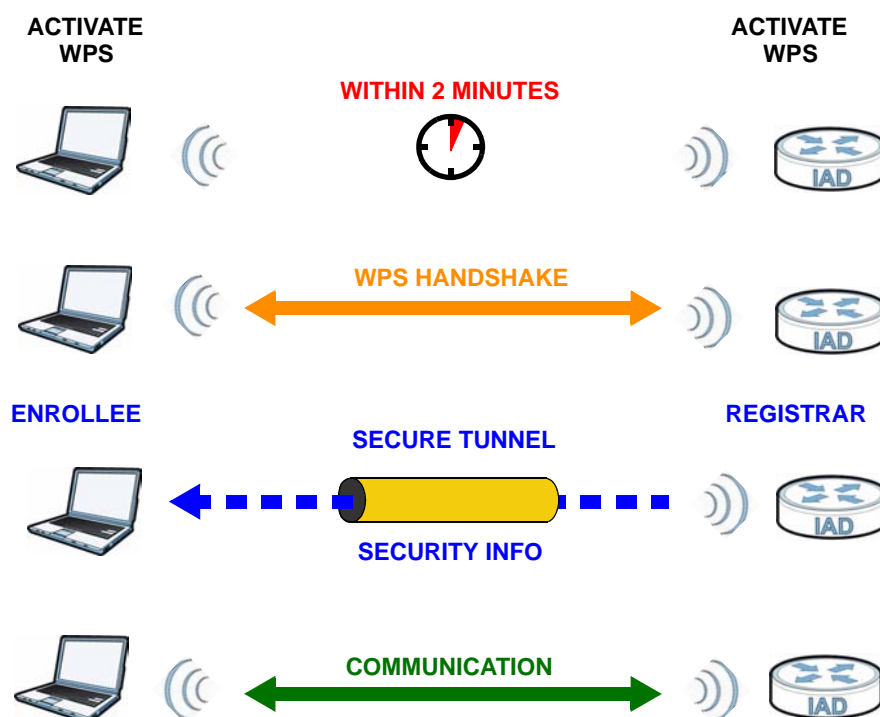


### 6.7.6.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

**Figure 44** How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

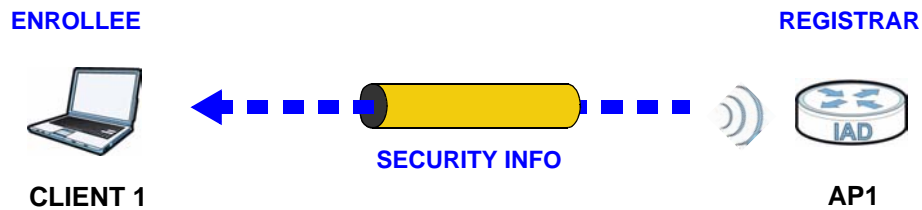
#### 6.7.6.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1**

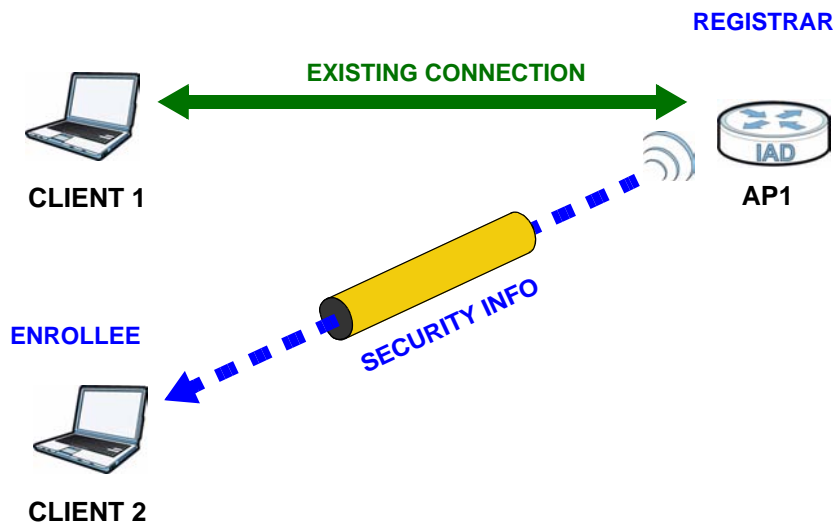
is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

**Figure 45** WPS: Example Network Step 1



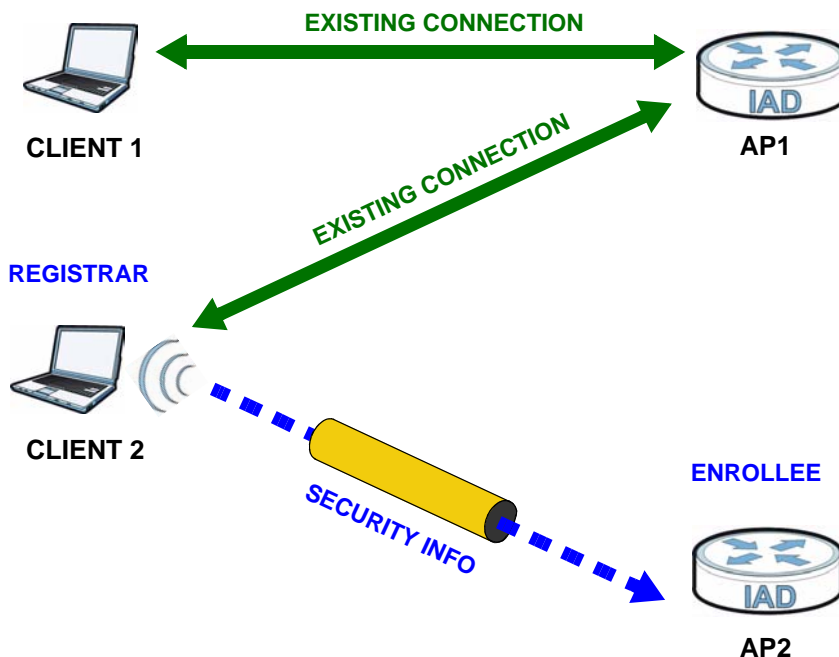
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

**Figure 46** WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

**Figure 47** WPS: Example Network Step 3



### 6.7.6.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

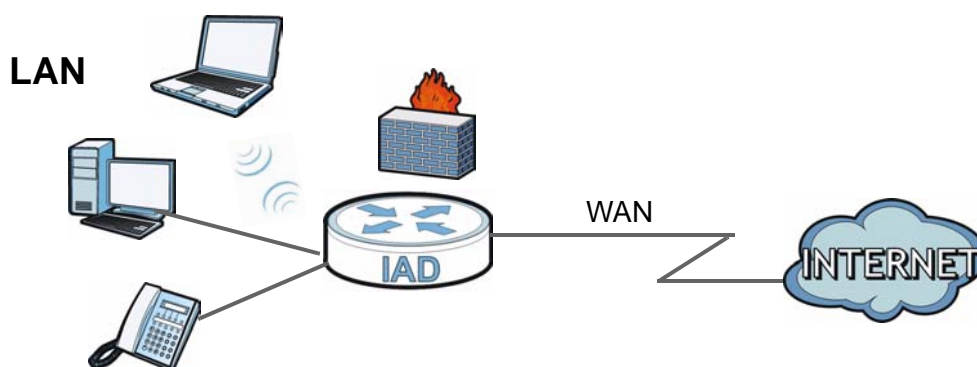


# Home Networking

## 7.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



### 7.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings ([Section 7.2 on page 152](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 7.3 on page 153](#)).
- Use the **UPnP** screen to enable UPnP ([Section 7.4 on page 155](#)).
- Use the **File Sharing** screen to enable file-sharing server ([Section 7.5 on page 155](#)).
- Use the **Media Server** screen to enable or disable the sharing of media files ([Section 7.6 on page 158](#)).
- Use the **Printer Server** screen to enable the print server ([Section 7.7 on page 159](#)).

### 7.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

#### 7.1.2.1 About LAN

##### IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

## Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

## DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

## DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

### 7.1.2.2 About UPnP

#### How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

#### Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

#### UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See [Section 7.9 on page 164](#) for examples of installing and using UPnP.

### 7.1.2.3 About File Sharing

#### Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

#### Shares

When settings are set to default, each USB device connected to the Device is given a folder, called a “share”. If a USB hard drive connected to the Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

#### File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Device supports File Allocation Table (FAT) and FAT32.

#### Common Internet File System

The Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

### 7.1.2.4 About Printer Server

#### Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

#### Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

#### TCP/IP

TCP/IP (Transmission Control Protocol/ Internet Protocol) is a set of communications protocols that most of the Internet runs on.

#### Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

### Supported OSs

Your operating system must support TCP/IP ports for printing and be compatible with the RAW (port 9100) protocol.

The following OSs support Device's printer sharing feature.

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.

## 7.2 The LAN Setup Screen

Click **Network Setting > Home Networking** to open the **LAN Setup** screen. Use this screen to set the Local Area Network IP address and subnet mask of your Device and configure the DNS server information that the Device sends to the DHCP client devices on the LAN.

**Figure 48** Network Setting > Home Networking > LAN Setup

**LAN IP Setup**

IP Address :

192.168.1.1

Subnet Mask :

255.255.255.0

(192.168.231.1 ~ 192.168.246.1 are reserved for VLAN.)

**DHCP Server State**

DHCP :

☒ Enable ☐ Disable

**IP Addressing Values**

IP Pool Starting Address :

192.168.1.33

Pool Size :

32

**DNS Values**

DNS Server 1 :

192.168.1.1

DNS Server 2 :

None

DNS Server 3 :

None

Apply

Cancel

The following table describes the fields in this screen.

**Table 28** Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	

**Table 28** Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DHCP	<p>Select <b>Enable</b> to have your Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients.</p> <p>If you select <b>Disable</b>, you need to manually configure the IP addresses of the computers and other devices on your LAN.</p> <p>When DHCP is used, the following fields need to be set.</p>
IP Addressing Values	
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Values	
DNS Server 1-3	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the Device's WAN IP address).</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 7.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

### 7.3.1 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Use this screen to change your Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

**Figure 49** Network Setting > Home Networking > Static DHCP

The screenshot shows a web interface for Static DHCP settings. At the top is a button labeled "Add new static lease". Below it is a table with the following columns: #, Status, Host Name, MAC Address, IP Address, and Reserve. The table contains one entry with the following values: # 1, Status (lightbulb icon), Host Name twpc13774-02, MAC Address 00:24:21:7e:20:96, IP Address 192.168.1.58, and Reserve (checkbox). At the bottom right are three buttons: Apply, Cancel, and Refresh.

#	Status	Host Name	MAC Address	IP Address	Reserve
1		twpc13774-02	00:24:21:7e:20:96	192.168.1.58	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 29** Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the Device.
Host Name	This field displays the client host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).  A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.
Refresh	Click <b>Refresh</b> to reload the DHCP table.

If you click **Add new static lease** in the **Static DHCP** screen, the following screen displays.

**Figure 50** Static DHCP: Add

The screenshot shows a web interface for adding a new static DHCP entry. It has two input fields: "MAC Address :" and "IP Address :". At the bottom right are two buttons: Apply and Back.

The following table describes the labels in this screen.

**Table 30** Static DHCP: Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.

**Table 30** Static DHCP: Add

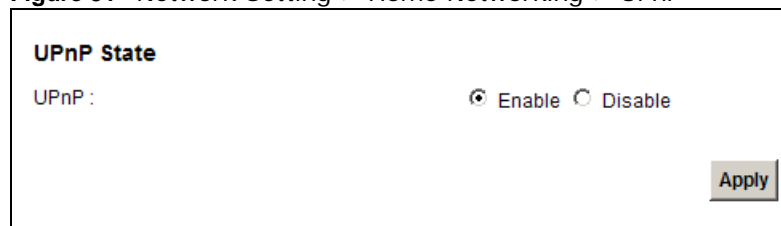
LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to exit this screen without saving.

## 7.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See [page 164](#) for more information on UPnP.

Use the following screen to configure the UPnP settings on your Device. Click **Network Setting > Home Networking > Static DHCP > UPnP** to display the screen shown next.

**Figure 51** Network Setting > Home Networking > UPnP


The following table describes the labels in this screen.

**Table 31** Network Settings > Home Networking > UPnP

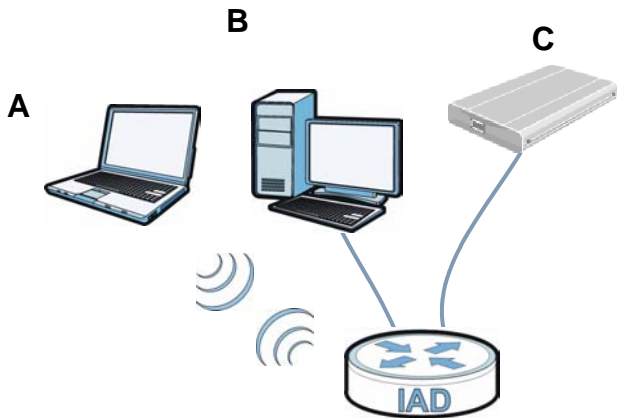
LABEL	DESCRIPTION
UPnP	Select <b>Enable</b> to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Device's IP address (although you must still enter the password to access the web configurator).
Apply	Click <b>Apply</b> to save your changes.

## 7.5 The File Sharing Screen

You can share files on a USB memory stick or hard drive connected to your Device with users on your network.

The following figure is an overview of the Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Device.

**Figure 52** File Sharing Overview



The Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

### 7.5.1 Before You Begin

Make sure the Device is connected to your network and turned on.

- 1 Connect the USB device to one of the Device's USB ports. Make sure the Device is connected to your network.
- 2 The Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the Device, see the troubleshooting for suggestions.

Use this screen to set up file sharing using the Device. To access this screen, click **Network Setting > Home Networking > File Sharing**.

**Figure 53** Network Setting > Home Networking > File Sharing

**Server Configuration**  
File Sharing Services(SMB) : ☒ Enable ☐ Disable

**Share Directory List**

#	Status	Share Name	Share Path	Share Description	Modify
1	<input checked="" type="checkbox"/>	USB_Storage	GENERIC_USB	USB_Storage	<input type="button" value="Edit"/> <input type="button" value="Delete"/>



Each field is described in the following table.

**Table 32** Network Setting > Home Networking > File Sharing

LABEL	DESCRIPTION
Server Configuration	
File Sharing Services (SMB)	Select <b>Enable</b> to activate file sharing through the Device.
Add new share	Click this to set up a new share on the Device.
#	Select the check box to make the share available to the network. Otherwise, clear this.
Status	This shows whether or not the share is available for sharing.
Share Name	This field displays the share name on the Device.
Share Path	This field displays the path for the share directories (folders) on the Device. These are the directories (folders) on your USB storage device.
Share Description	This field displays information about the share.
Modify	Click the <b>Edit</b> icon to change the settings of an existing share. Click the <b>Delete</b> icon to delete this share in the list.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 7.5.2 Add/Edit File Sharing

Use this screen to set up a new share or edit an existing share on the Device. Click **Add new share** in the **File Sharing** screen or click the **Edit** icon next to an existing share.

**Figure 54** File Sharing: Add/Edit

Each field is described in the following table.

**Table 33** File Sharing: Add/Edit

LABEL	DESCRIPTION
Volume	Select the volume in the USB storage device that you want to add as a share in the Device.  This field is read-only when you are editing the share.
Share Path	Manually enter the file path for the share, or click the <b>Browse</b> button and select the folder that you want to add as a share.  This field is read-only when you are editing the share.
Description	You can either enter a short description of the share, or leave this field blank.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen.

# 7.6 The Media Server Screen

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your Device (without having to copy them to another computer). The Device can function as a DLNA-compliant media server. The Device streams files to DLNA-compliant media clients (like Windows Media Player). The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

The Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

To change your Device's media server settings, click **Network Setting > Home Networking > Media Server**. The screen appears as shown.

**Figure 55** Network Setting > Home Networking > Media Server



The following table describes the labels in this menu.

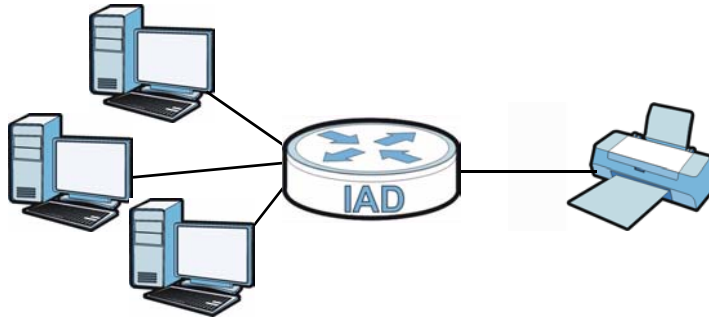
**Table 34** Network Setting > Home Networking > Media Server

LABEL	DESCRIPTION
Enable Media Server	Check this to have the Device function as a DLNA-compliant media server. Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares.
Apply	Click <b>Apply</b> to save your changes.

## 7.7 The Printer Server Screen

The Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the Device and then configuring a TCP/IP port on the computers connected to your network.

**Figure 56** Sharing a USB Printer



### 7.7.1 Before You Begin

To configure the print server you need the following:

- Your Device must be connected to your computer and any other devices on your network. The USB printer must be connected to your Device.
- A USB printer with the driver already installed on your computer.
- The computers on your network must have the printer software already installed before they can create a TCP/IP port for printing via the network. Follow your printer manufacturers instructions on how to install the printer software on your computer.

**Note:** Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the Device instead.

Use this screen to enable or disable sharing of a USB printer via your Device.

To access this screen, click **Network Setting > Home Networking > Printer Server**.

**Figure 57** Network Setting > Home Networking > Printer Server

**Print Server Configuration**

Print Server : ☒ Enable ☐ Disable

Apply
Cancel

The following table describes the labels in this menu.

**Table 35** Network Setting > Home Networking > Print Server

LABEL	DESCRIPTION
Printer Server	Select <b>Enable</b> to have the Device share a USB printer.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

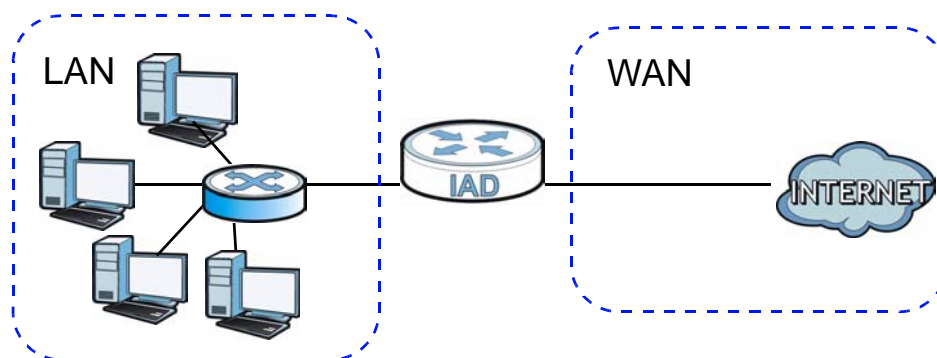
## 7.8 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

### LANs, WANs and the Device

The actual physical connection determines whether the Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

**Figure 58** LAN and WAN IP Addresses



### DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Device as a DHCP server or disable it. When configured as a server, the Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

### IP Pool Setup

The Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

## LAN TCP/IP

The Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

### IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

### Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

**Note:** Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

## Device Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the Device print server.

**Table 36** Compatible USB Printers

BRAND	MODEL
Brother	MFC7420
CANON	BJ F9000
CANON	i320
CANON	PIXMA MP450
CANON	PIXMA MP730
CANON	PIXMA MP780
CANON	PIXMA MP830
CANON	PIXUS ip2500
CANON	PIXMA ip4200
CANON	PIXMA ip5000
CANON	PIXUS 990i
EPSON	CX3500
EPSON	CX3900
EPSON	EPL-5800
EPSON	EPL-6200L
EPSON	LP-2500
EPSON	LP-8900
EPSON	RX 510
EPSON	RX 530
EPSON	Stylus 830U
EPSON	Stylus 1270
EPSON	Stylus C43UX
EPSON	Stylus C60
EPSON	Stylus Color 670
HP	Deskjet 5550
HP	Deskjet 5652
HP	Deskjet 830C
HP	Deskjet 845C
HP	Deskjet 1125C
HP	Deskjet 1180C

**Table 36** Compatible USB Printers (continued)

<b>BRAND</b>	<b>MODEL</b>
HP	Deskjet 1220C
HP	Deskjet F4185
HP	Laserjet 1022
HP	Laserjet 1200
HP	Laserjet 2200D
HP	Laserjet 2420
HP	Color Laserjet 1500L
HP	Laserjet 3015
HP	Officejet 4255
HP	Officejet 5510
HP	Officejet 5610
HP	Officejet 7210
HP	Officejet Pro L7380
HP	Photosmart 2610
HP	Photosmart 3110
HP	Photosmart 7150
HP	Photosmart 7830
HP	Photosmart C5280
HP	Photosmart D5160
HP	PSC 1350
HP	PSC 1410
IBM	Infoprint 1332
LEXMARK	Z55
LEXMARK	Z705
OKI	B4350
SAMSUNG	ML-1710
SAMSUNG	SCX-4016

## 7.9 Installing UPnP in Windows Example

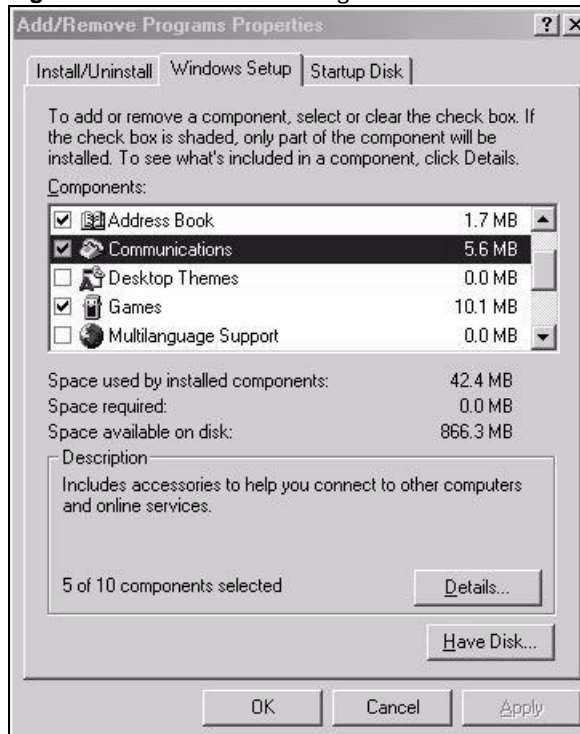
This section shows how to install UPnP in Windows Me and Windows XP.

### Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

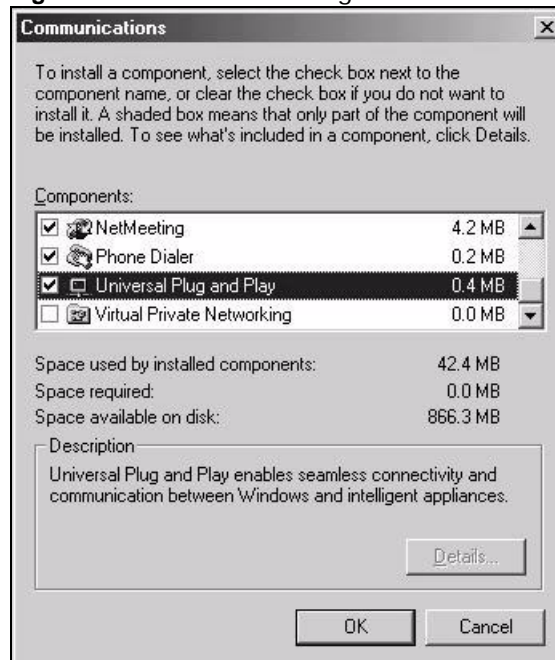
**Figure 59** Add/Remove Programs: Windows Setup: Communication





- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

**Figure 60** Add/Remove Programs: Windows Setup: Communication: Components



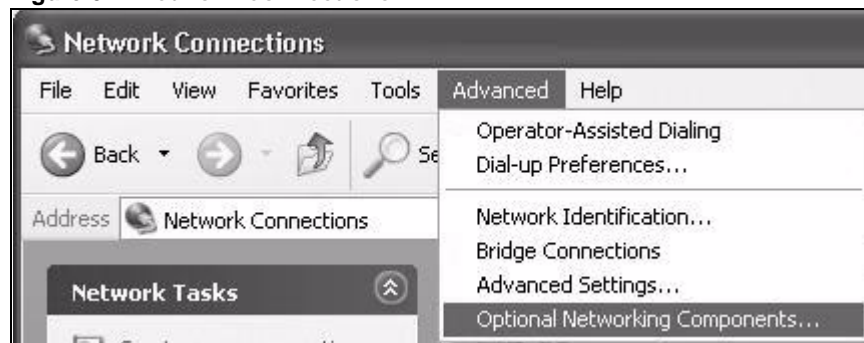
- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

### Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

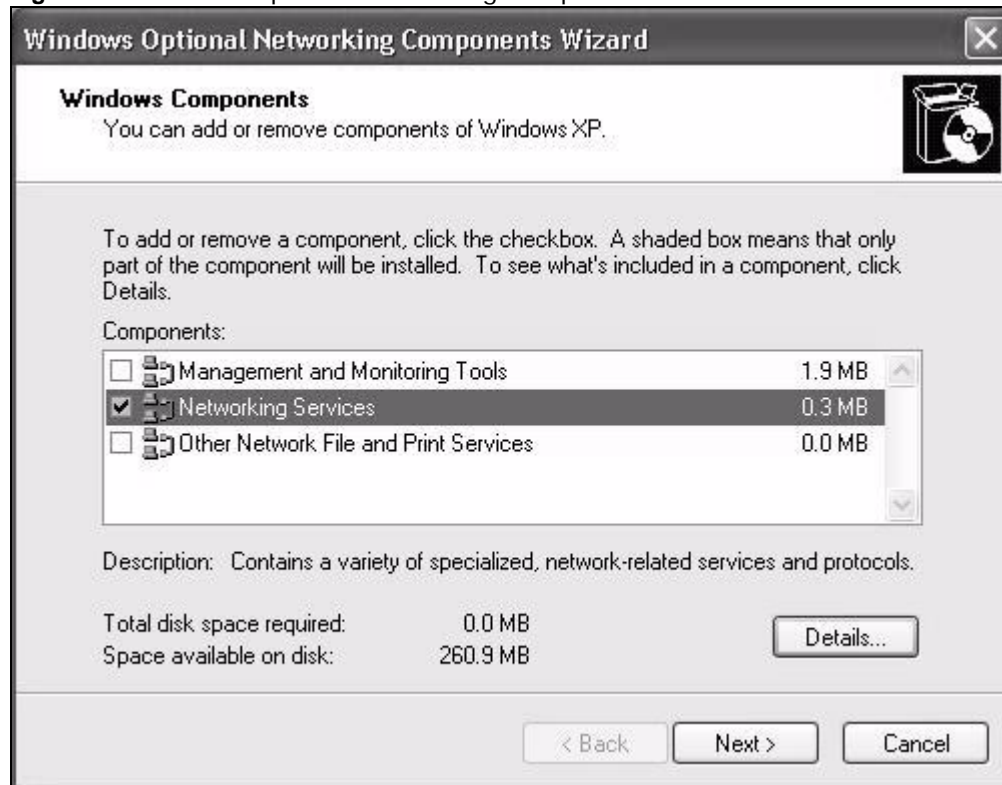
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**

**Figure 61** Network Connections



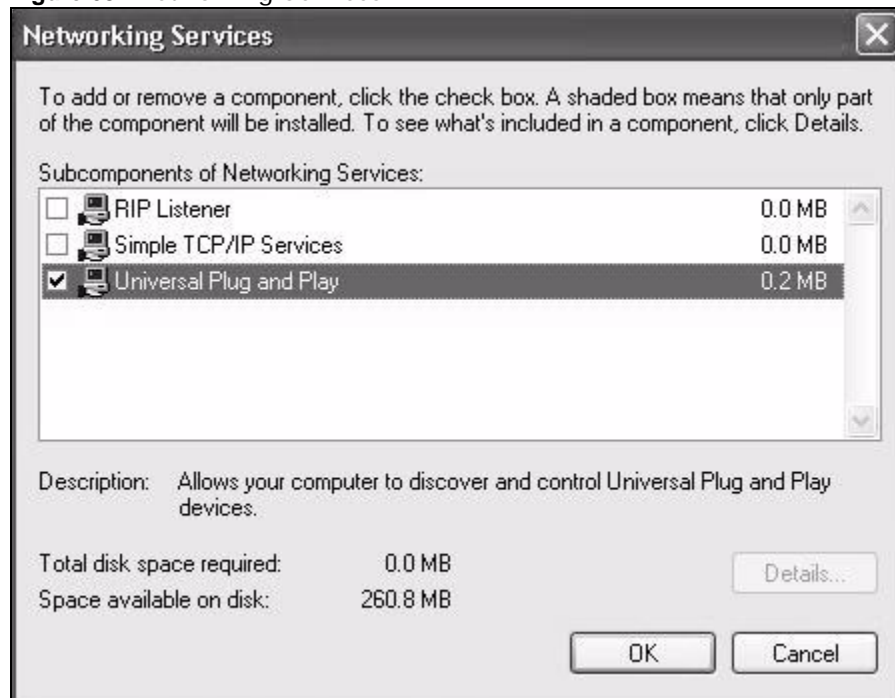
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 62** Windows Optional Networking Components Wizard



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

**Figure 63** Networking Services



- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

## 7.10 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Device.

Make sure the computer is connected to a LAN port of the Device. Turn on your computer and the Device.

### Auto-discover Your UPnP-enabled Network Device

- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.

**Figure 64** Network Connections



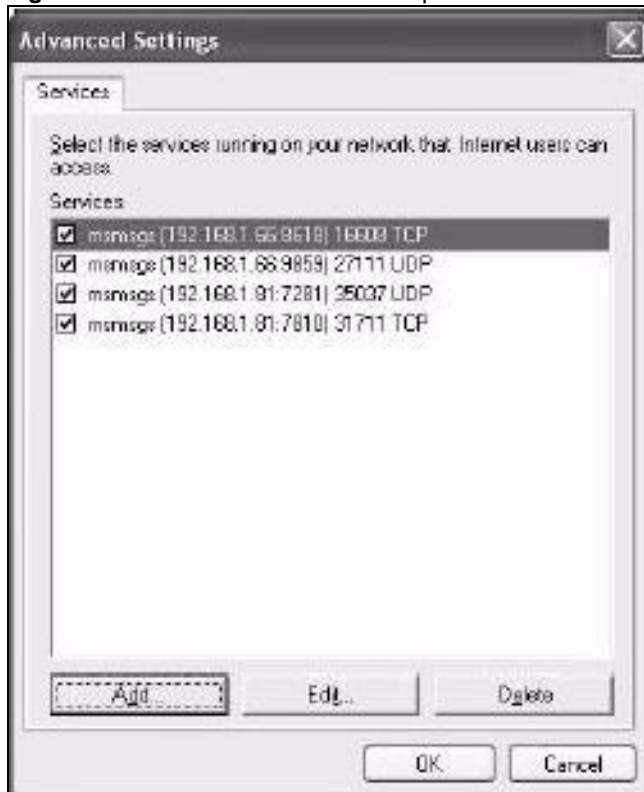
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

**Figure 65** Internet Connection Properties

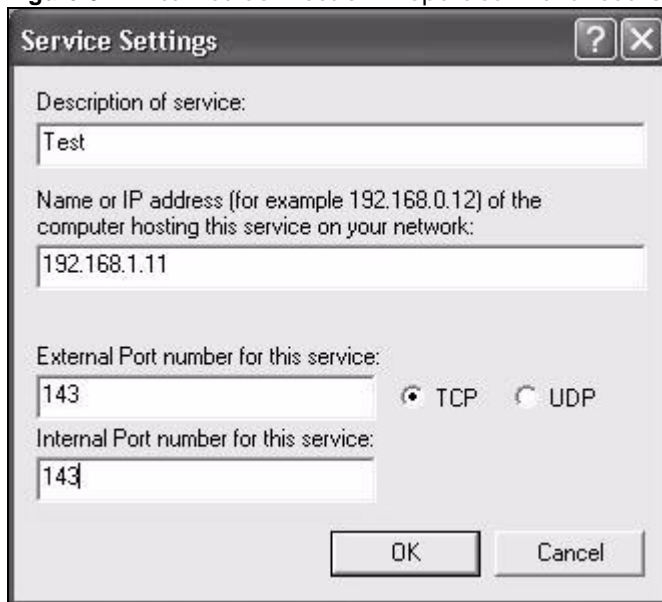


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 66** Internet Connection Properties: Advanced Settings



**Figure 67** Internet Connection Properties: Advanced Settings: Add



- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

**Figure 68** System Tray Icon



- 7 Double-click on the icon to display your current Internet connection status.

**Figure 69** Internet Connection Status



### Web Configurator Easy Access

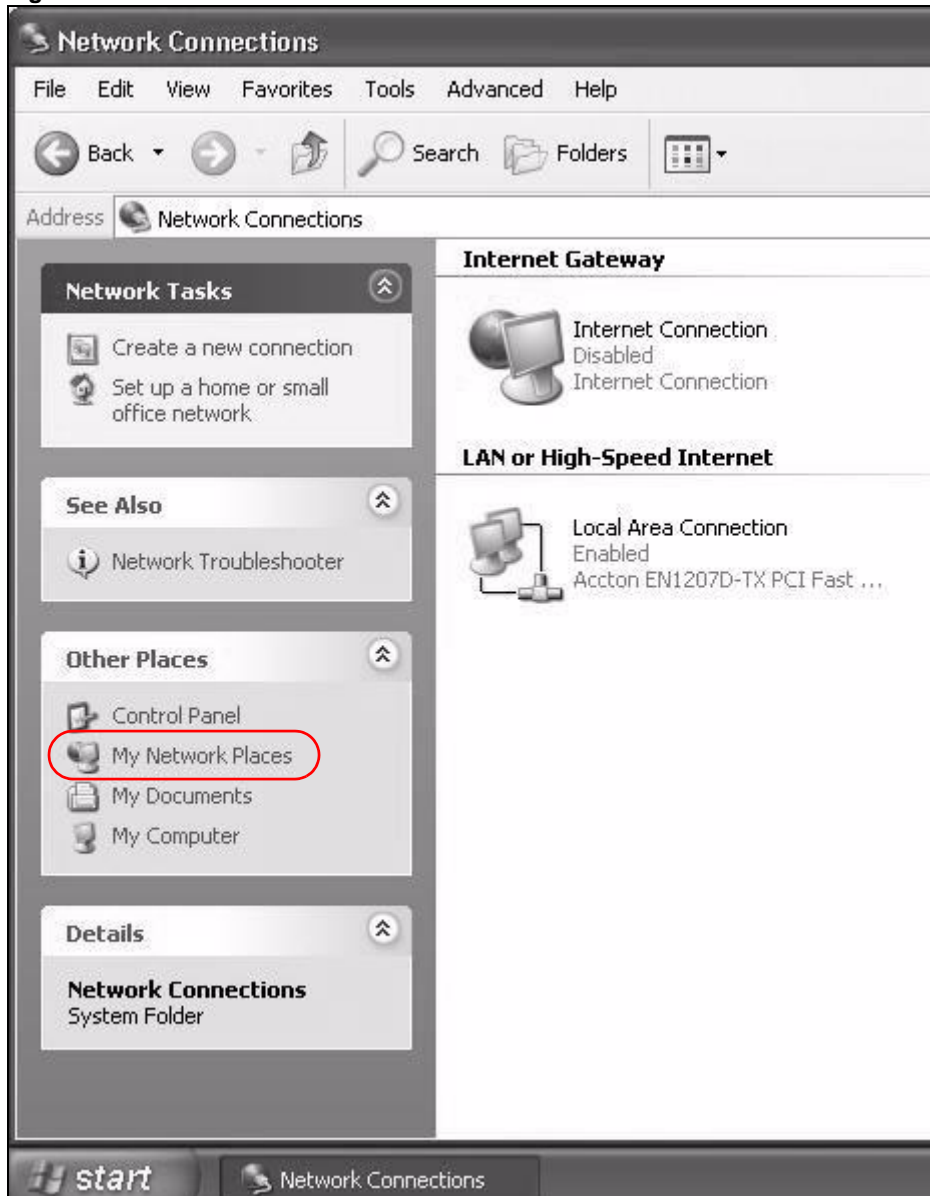
With UPnP, you can access the web-based configurator on the Device without finding out the IP address of the Device first. This comes helpful if you do not know the IP address of the Device.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

- 3 Select **My Network Places** under **Other Places**.

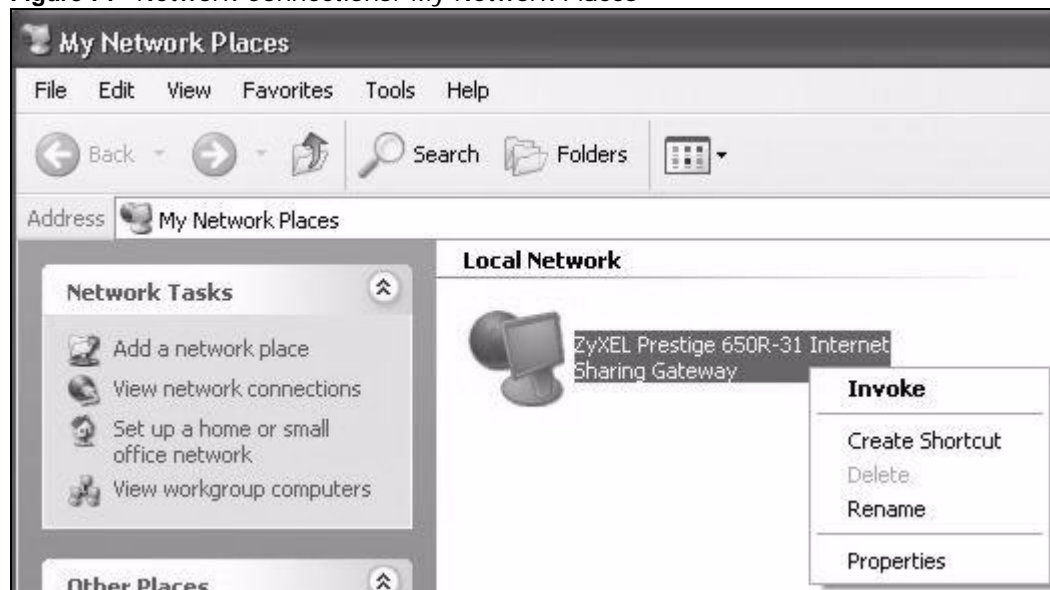
**Figure 70** Network Connections



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

- 5 Right-click on the icon for your Device and select **Invoke**. The web configurator login screen displays.

**Figure 71** Network Connections: My Network Places



- 6 Right-click on the icon for your Device and select **Properties**. A properties window displays with basic information about the Device.

**Figure 72** Network Connections: My Network Places: Properties: Example





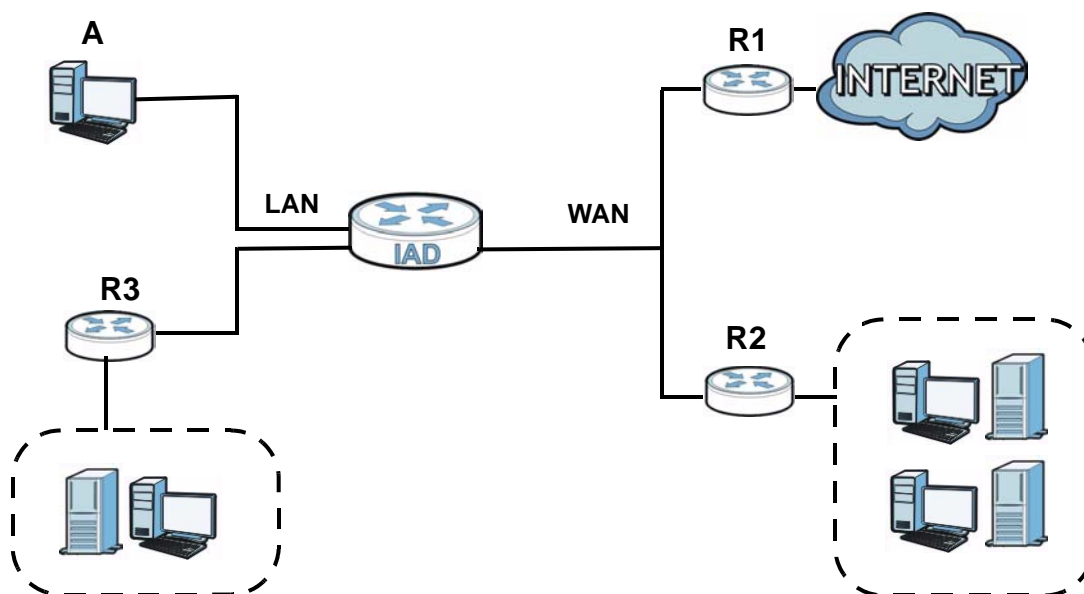
# Routing

## 8.1 Overview

The Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Device's LAN interface. The Device routes most traffic from **A** to the Internet through the Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.


**Figure 73** Example of Static Routing Topology



## 8.2 Configuring Static Route

Use this screen to view and configure IP static routes on the Device. Click **Network Setting > Static Route** to open the following screen.

**Figure 74** Network Setting > Static Route

Add New Static Route								
#	Active	Status	Name	Destination IP	Gateway	Subnet Mask	Interface	Modify
1			test1	192.168.0.0		255.255.0.0	EtherWAN1	 

The following table describes the labels in this screen.

**Table 37** Network Setting > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Device.
#	This is the number of an individual static route.
Active	This indicates whether the rule is active or not.  A yellow bulb signifies that this static route is active. A gray bulb signifies that this static route is not active.
Status	This shows whether the static route is currently in use or not. A yellow bulb signifies that this static route is in use. A gray bulb signifies that this static route is not in use.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Modify	Click the <b>Edit</b> icon to go to the screen where you can set up a static route on the Device.  Click the <b>Delete</b> icon to remove a static route from the Device.

## 8.2.1 Add/Edit Static Route

Click **add new Static Route** in the **Routing** screen or click the **Edit** icon next to a rule. The following screen appears. Use this screen to configure the required information for a static route.

**Figure 75** Routing: Add/Edit

☐ Active

Route Name :

Destination IP Address :

IP Subnet Mask :

Gateway IP Address :

Bound Interface ☒ EtherWAN1

**Note :**

The Destination IP Address and IP Subnet Mask fields must be matched; e.g. host/255.255.255.255 or subnet/255.255.255.0.

**Apply** **Back**

The following table describes the labels in this screen.

**Table 38** Routing: Add/Edit

LABEL	DESCRIPTION
Active	Click this to activate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	<p>You can decide if you want to forward packets to a gateway IP address or a bound interface.</p> <p>If you want to configure <b>Gateway IP Address</b>, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.</p>
Bound Interface	<p>You can decide if you want to forward packets to a gateway IP address or a bound interface.</p> <p>If you want to configure <b>Bound Interface</b>, select the check box and choose an interface through which the traffic is sent. You must have the WAN interface(s) already configured in the <b>Broadband</b> screen.</p>
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to exit this screen without saving.



# Quality of Service (QoS)

## 9.1 Overview

This chapter discusses the Device's **QoS** screens. Use these screens to set up your Device to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. QoS allows the Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

The Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

Note: The Device has built-in configurations for Voice over IP (IP). The Quality of Service (QoS) feature does not affect VoIP traffic.

- See [Section 9.6 on page 187](#) for advanced technical information on SIP.

### 9.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable QoS, set the bandwidth, and allow the Device to automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length ([Section 9.2 on page 178](#)).
- Use the **Queue Setup** screen to configure QoS queue assignment ([Section 9.3 on page 180](#)).
- Use the **Class Setup** screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow ([Section 9.4 on page 181](#)).
- Use the **Monitor** screen to view the Device's QoS-related packet statistics ([Section 9.5 on page 186](#)).

### 9.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

## QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

## Tagging and Marking

In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

## 9.2 The QoS General Screen

Use this screen to enable or disable QoS, set the bandwidth, and select to have the Device automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length.

Click **Network Setting > QoS** to open the **General** screen.

**Figure 76** Network Setting > QoS > General

☒ Active QoS

WAN Managed Upstream Bandwidth :  (kbps)

Traffic priority will be automatically assigned by

**Note :**

You can assign the upstream bandwidth manually.  
If the field is empty, the CPE set the value automatically.  
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.

The following table describes the labels in this screen.

**Table 39** Network Setting > QoS > General

LABEL	DESCRIPTION
Active QoS	<p>Select the check box to turn on QoS to improve your network performance.</p> <p>You can give priority to traffic that the Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.</p>
WAN Managed Upstream Bandwidth	<p>Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 1000 kbps if your Internet connection has an upstream transmission speed of 1 Mbps.</p> <p>Setting this number higher than the interface's actual transmission speed will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth.</p> <p>If you set this number lower than the interface's actual transmission speed, the Device will not use some of the interface's available bandwidth.</p> <p>Leave this field blank to have the Device set this value automatically.</p>
Traffic priority will be automatically assigned by	<p>These fields are ignored if upstream traffic matches a class you configured in the <b>Class Setup</b> screen.</p> <p>If you select <b>Ethernet Priority</b>, <b>IP Precedence</b> or <b>Packet Length</b> and traffic does not match a class configured in the <b>Class Setup</b> screen, the Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence or packet length.</p> <p>See <a href="#">Section 9.6.1 on page 187</a> for more information.</p>
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 9.3 The Queue Setup Screen

Use this screen to configure QoS queue assignment. Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

**Figure 77** Network Setting > QoS > Queue Setup

<b>Add new Queue</b>								
#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit (kbps)	Modify
1		WAN_Default_Queue	WAN	4	1	DT		
2		LAN_Default_Queue	LAN	4	1	DT		
3		Fast	WAN	7	3	DT		
4		Active user	WAN	5	3	DT		
5		Passive user	WAN	3	3	DT		
6		Slow	WAN	1	3	DT		

**Note :**  
Maximum 8 user configurable entries.

The following table describes the labels in this screen.

**Table 40** Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add new Queue	Click this to create a new entry.
#	This is the index number of this entry.
Status	This indicates whether the queue is active or not.  A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used by the Device.
Rate Limit (kbps)	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the <b>Edit</b> icon to edit the queue.  Click the <b>Delete</b> icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.



### 9.3.1 Add/Edit a QoS Queue

Use this screen to configure a queue. Click **Add new queue** in the **Queue Setup** screen or the **Edit** icon next to an existing queue.

**Figure 78** Queue Setup: Add/Edit

The following table describes the labels in this screen.

**Table 41** Queue Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	This shows the interface of this queue.
Priority	Select the priority level (from 1 to 7) of this queue.  The larger the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 15) of this queue.  If two queues have the same priority level, the Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen without saving.

## 9.4 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Class Setup** to open the following screen.

**Figure 79** Network Setting > QoS > Class Setup

Add new Classifier								
Order	Status	Class Name	Classification Criteria	Forward to	DSCP Mark	802.1P Mark	To Queue	Modify
1		From device	Interface: Local	UnChange	UnChange	UnChange	Fast	
2		ICMP	Ether Type: IP Protocol: ICMP	UnChange	UnChange	UnChange	Fast	
3		HTTP	Ether Type: IP Protocol: TCP Destination Port: 80	UnChange	UnChange	UnChange	Active user	
4		HTTP-Proxy	Ether Type: IP Protocol: TCP Destination Port: 8080	UnChange	UnChange	UnChange	Active user	
5		HTTPS	Ether Type: IP Protocol: TCP Destination Port: 443	UnChange	UnChange	UnChange	Active user	
6		LAN or WLAN TCP po...	Ether Type: IP Protocol: TCP Destination Port: 1024:...	UnChange	UnChange	UnChange	Slow	
7		LAN or WLAN UDP po...	Ether Type: IP Protocol: UDP Destination Port: 1024:...	UnChange	UnChange	UnChange	Slow	

The following table describes the labels in this screen.

**Table 42** Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
Order	This field displays the order number of the classifier.
Status	This indicates whether the classifier is active or not.  A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward to	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1p Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the <b>Edit</b> icon to edit the classifier.  Click the <b>Delete</b> icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

## 9.4.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to an existing classifier to configure it.

**Figure 80** Class Setup: Add/Edit

**Class Configuration**

Active : ☒  
Class Name :   
Classification Order :   
Forward To Interface :   
DSCP Mark :  (0~63)  
802.1P : Mark :   
To Queue :

**Criteria Configuration**  
Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

**Basic**

☐ From Interface   
☐ Ether Type

**Source**

☐ MAC Address  MAC Mask  ☐ Exclude  
☐ IP Address  IP Subnet Mask  ☐ Exclude  
☐ Port Range  ~  (1~65535) ☐ Exclude

**Destination**

☐ MAC Address  MAC Mask  ☐ Exclude  
☐ IP Address  IP Subnet Mask  ☐ Exclude  
☐ Port Range  ~  (1~65535) ☐ Exclude

**Others**

☐ 802.1P  ☐ Exclude  
☐ IP Protocol   ☐ Exclude  
☐ IP Packet Length  ~  (46~1504) ☐ Exclude  
☐ DSCP  ☐ Exclude  
☐ TCP ACK ☐ Exclude  
☐ DHCP  ☐ Exclude  
Class ID  (String)  
☐ Service  ☐ Exclude

The following table describes the labels in this screen.

**Table 43** Class Setup: Add/Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable this classifier.
Class Name	Enter a descriptive name of up to 32 printable English keyboard characters, including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking <b>Apply</b> . Select <b>Last</b> to put this rule in the back of the classifier list.

**Table 43** Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select <b>Unchange</b> , the Device forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the <b>Ether Type</b> check box in <b>Criteria Configuration-Basic</b> section.  If you select <b>Mark</b> , enter a DSCP value with which the Device replaces the DSCP field in the packets.  If you select <b>Unchange</b> , the Device keep the DSCP field in the packets.
802.1p Mark	Select a priority level with which the Device replaces the IEEE 802.1p priority field in the packets.  If you select <b>Unchange</b> , the Device keep the 802.1p priority field in the packets.
To Queue	Select a queue that applies to this class.  You should have configured a queue in the <b>Queue Setup</b> screen already.
Criteria Configuration	
Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select whether the traffic class comes from the LAN or a wireless interface.
Ether Type	Select a predefined application to configure a class for the matched traffic.  If you select <b>IP</b> , you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type.  If you select <b>8021Q</b> , you can configure an 802.1p priority level and VLAN ID in the <b>Others</b> section.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.  Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
Port Range	If you select <b>TCP</b> or <b>UDP</b> in the <b>IP Protocol</b> field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.

**Table 43** Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.  Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
Port Range	If you select <b>TCP</b> or <b>UDP</b> in the <b>IP Protocol</b> field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
802.1p	This field is available only when you select <b>802.1Q</b> in the <b>Ether Type</b> field.  Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
IP Protocol	This field is available only when you select <b>IP</b> in the <b>Ether Type</b> field.  Select this option and select the protocol (service type) from <b>TCP</b> or <b>UDP</b> . If you select <b>User defined</b> , enter the protocol (service type) number.
IP Packet Length	This field is available only when you select <b>IP</b> in the <b>Ether Type</b> field.  Select this option and enter the minimum and maximum packet length (from 46 to 1504) in the fields provided.
DSCP	This field is available only when you select <b>IP</b> in the <b>Ether Type</b> field.  Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
TCP ACK	This field is available only when you select <b>IP</b> in the <b>Ether Type</b> field.  If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
DHCP	This field is available only when you select <b>IP</b> in the <b>Ether Type</b> field, and <b>UDP</b> in the <b>IP Protocol</b> field.  Select this option and select a DHCP option.  If you select <b>Vendor Class ID (DHCP Option 60)</b> , enter the <b>Class ID</b> of the matched traffic, such as the type of the hardware or firmware.  If you select <b>ClientID (DHCP Option 61)</b> , enter the <b>Type</b> of the matched traffic and <b>Client ID</b> of the DHCP client.  If you select <b>User Class ID (DHCP Option 77)</b> , enter the <b>User Class Data</b> , which is a string that identifies the user's category or application type in the matched DHCP packets.  If you select <b>VendorSpecificIntro (DHCP Option 125)</b> , enter the <b>Enterprise Number</b> of the software of the matched traffic and <b>Vendor Class Data</b> used by all the DHCP clients.
Service	Select the service classification of the traffic.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.

**Table 43** Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen without saving.

## 9.5 The QoS Monitor Screen

To view the Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

**Figure 81** Network Setting > QoS > Monitor

The screenshot shows the 'Monitor' screen with a 'Refresh Interval' dropdown set to 'No Refresh'. Under 'Status', there are two sections: 'Interface Monitor' and 'Queue Monitor'.

**Interface Monitor**

#	Name	Pass Rate(bps)
1	ptm0.3900	

**Queue Monitor**

#	Name	Interface	Pass Rate(bps)	Drop Rate(bps)
1	WAN_Default_Queue	WAN	0	0
2	LAN_Default_Queue	LAN	0	0
3	Fast	WAN	0	0
4	Active user	WAN	0	0
5	Passive user	WAN	0	0
6	Slow	WAN	0	0

The following table describes the labels in this screen.

**Table 44** Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Monitor	
Refresh Interval	Select how often you want the Device to update this screen. Select <b>No Refresh</b> to stop refreshing statistics.
Status	
#	This is the index number of the entry.
Name	This shows the name of the WAN interface on the Device.
Pass Rate (bps)	This shows how much traffic (bps) forwarded to this interface are transmitted successfully.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate (bps)	This shows how much traffic (bps) assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how much traffic (bps) assigned to this queue are dropped.

## 9.6 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

### 9.6.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

**Table 45** IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

### 9.6.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

### 9.6.3 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to

negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

## DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.



# Network Address Translation (NAT)

## 10.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

### 10.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network ([Section 10.2 on page 190](#)).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use ([Section on page 192](#)).

### 10.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

#### Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

#### NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

#### Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

## Finding Out More

See [Section 10.4 on page 193](#) for advanced technical information on NAT.

## 10.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

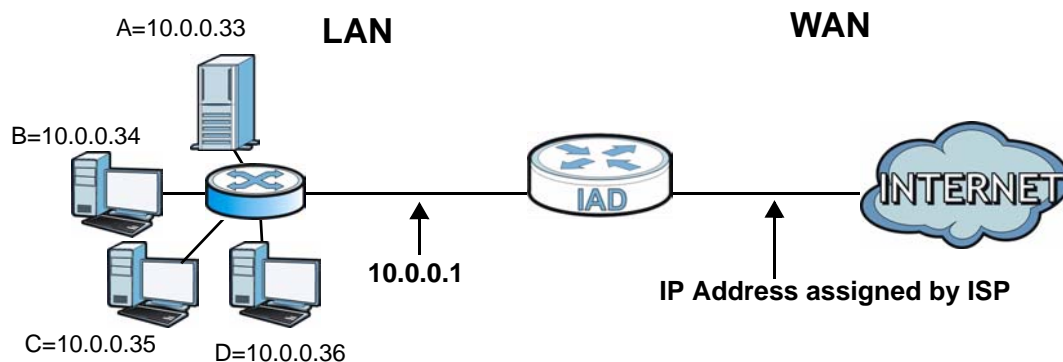
The most often used port numbers and services are shown in [Appendix E on page 359](#). Please refer to RFC 1700 for further information about port numbers.

**Note:** Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

### Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 10.0.0.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 82** Multiple Servers Behind NAT Example



### 10.2.1 The Port Forwarding Screen

Click **Network Setting > NAT** to open the **Port Forwarding** screen.

See [Appendix E on page 359](#) for port numbers commonly used for particular services.

**Figure 83** Network Setting > NAT > Port Forwarding

The screenshot shows a web interface for configuring NAT port forwarding. At the top left is a button labeled 'Add new rule'. Below it is a table with the following columns: #, Status, Service Name, WAN Interface, Start Port, End Port, Translation Start Port, Translation End Port, Server IP Address, Protocol, and Modify. There is one row in the table with the following values: 1, a yellow lightbulb icon, User Defined, EtherWAN1, 21, 21, 21, 21, 192.168.1.6, TCP, and edit/delete icons. Below the table is a 'Note' section with a document icon and the text: 'The TCP port 30005 is reserved for TR069 connection request port.'

#	Status	Service Name	WAN Interface	Start Port	End Port	Translation Start Port	Translation End Port	Server IP Address	Protocol	Modify
1		User Defined	EtherWAN1	21	21	21	21	192.168.1.6	TCP	

**Note :**  
The TCP port 30005 is reserved for TR069 connection request port.

The following table describes the fields in this screen.

**Table 46** Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add new rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not.  A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows <b>User Defined</b> if you manually added a service. You can change this by clicking the edit icon.
WAN Interface	This shows the WAN interface through which the service is forwarded.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Protocol	This shows the IP protocol supported by this virtual server, whether it is <b>TCP</b> , <b>UDP</b> , or <b>TCP/UDP</b> .
Modify	Click the <b>Edit</b> icon to edit the port forwarding rule.  Click the <b>Delete</b> icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 10.2.2 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Click **Add new rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

**Figure 84** Port Forwarding: Add/Edit

The screenshot shows a web-based configuration interface for port forwarding. It includes a checkbox for 'Enable', a text field for 'Service Name' with the value 'User Defined', a dropdown for 'WAN Interface' set to 'EtherWAN1', and text fields for 'Start Port', 'End Port', 'Translation Start Port', and 'Translation End Port', all containing the value '21'. There is also a text field for 'Server IP Address' with the value '192.168.1.6' and a dropdown for 'Protocol' set to 'TCP'. At the bottom right, there are 'Apply' and 'Back' buttons.

The following table describes the labels in this screen.

**Table 47** Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Enable	This is available only in the <b>Edit</b> screen. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Start Port	Enter the original destination port for the packets.  To forward only one port, enter the port number again in the <b>External End Port</b> field.  To forward a series of ports, enter the start port number here and the end port number in the <b>External End Port</b> field.
End Port	Enter the last port of the original destination port range.  To forward only one port, enter the port number in the <b>External Start Port</b> field above and then enter it again in this field.  To forward a series of ports, enter the last port number in a series that begins with the port number in the <b>External Start Port</b> field above.
Translation Start Port	This shows the port number to which you want the Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol Type	Select the protocol supported by this virtual server. Choices are <b>TCP</b> , <b>UDP</b> , or <b>TCP/UDP</b> .

**Table 47** Port Forwarding: Add/Edit (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen without saving.

## 10.3 The Sessions Screen

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use.

Click **Network Setting > NAT > Sessions** to display the following screen.

**Figure 85** Network Setting > NAT > Sessions

MAX NAT Sessions Per Host :  (512 - 20480)

Apply Cancel

The following table describes the fields in this screen.

**Table 48** Network Setting > NAT > Sessions

LABEL	DESCRIPTION
MAX NAT Session	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have.  If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 10.4 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

### 10.4.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 49** NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

## 10.4.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

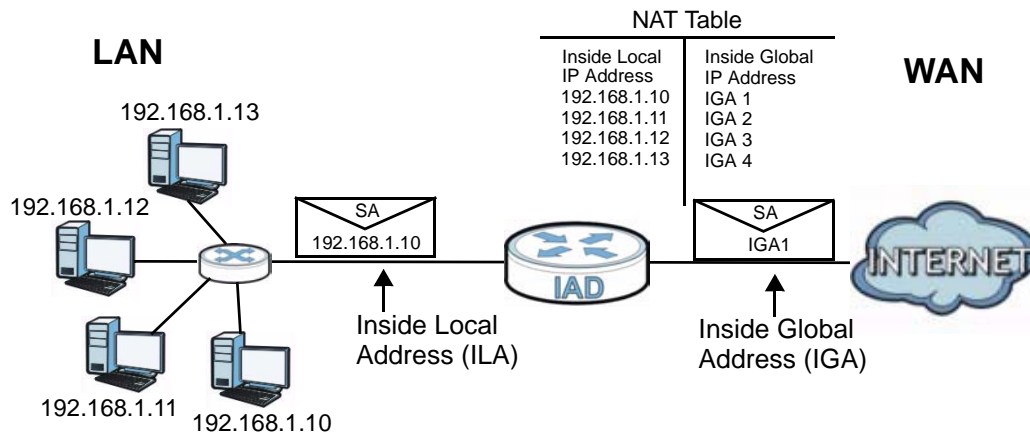
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a Telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

## 10.4.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The

Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

**Figure 86** How NAT Works







## Dynamic DNS

### 11.1 Overview

This chapter discusses how to configure your Device to use Dynamic DNS.

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in applications such as NetMeeting and CU-SeeMe). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with [www.dyndns.org](http://www.dyndns.org). This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

#### 11.1.1 What You Need To Know

##### DYNDNS Wildcard

Enabling the wildcard feature for your host causes \*.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

### 11.2 The Dynamic DNS Screen

Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Device. To change your Device's DDNS, click **Network Setting > DNS**. The screen appears as shown.

**Figure 87** Network Setting > DNS

**Dynamic DNS Configuration**

☐ Active Dynamic DNS

Service Provider : WWW.DynDNS.ORG

Dynamic DNS Type : Dynamic DNS

Host Name :  (1 to 255 characters)

User Name :  (1 to 255 characters)

Password :  (1 to 63 characters)

Apply Cancel

The following table describes the fields in this screen.

**Table 50** Network Setting > DNS

LABEL	DESCRIPTION
Dynamic DNS Configuration	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

# Firewall

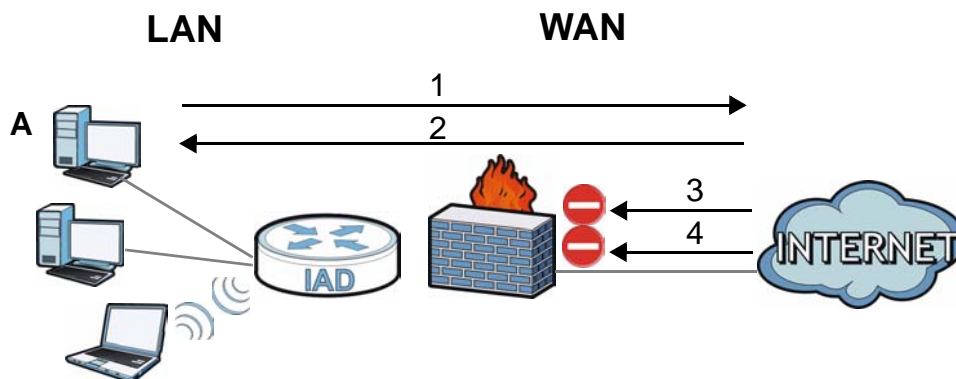
## 12.1 Overview

Use the Device firewall screens to enable and configure the firewall that protects your Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- Allows traffic that originates from your LAN and WLAN computers to go to all other networks.
- Blocks traffic that originates on other networks from going to the LAN and WLAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

**Figure 88** Default Firewall Action



### 12.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable the Device's firewall ([Section 12.2 on page 200](#)).
- Use the **Services** screen to view the configured firewall rules and add, edit or remove a firewall rule ([Section 12.3 on page 201](#)).

### 12.1.2 What You Need to Know

#### Firewall

The Device's firewall feature physically separates the LAN/WLAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is designed to protect against Denial of Service (DoS) attacks when activated. The Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet.

The Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The Device is installed between the LAN/WLAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The Device has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

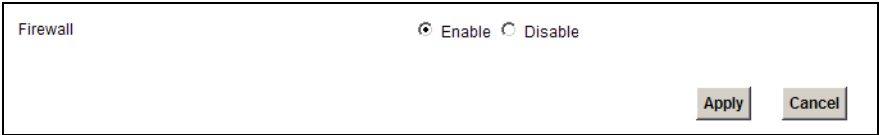
Finding Out More

See [Section 12.4 on page 202](#) for advanced technical information on firewall.

12.2 The General Screen

Use this screen to enable or disable the Device's firewall. Click **Security > Firewall** to open the **General** screen.

Figure 89 Security > Firewall > General



The following table describes the labels in this screen.

Table 51 Security > Firewall > General

LABEL	DESCRIPTION
Firewall	Select <b>Enable</b> to activate the firewall. The Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 12.3 The Services Screen

Use this screen to enable service blocking and to maintain the list of services you want to block. To access this screen, click **Security > Firewall > Services**.

Note: These rules specify which computers on the LAN can access which computers or services on the WAN.

**Figure 90** Security > Firewall > Services

Each field is described in the following table.

**Table 52** Security > Firewall > Services

LABEL	DESCRIPTION
LAN-to-WAN Services Blocking	Select <b>Enable</b> to activate service blocking.
Available Services	<p>This is a list of pre-defined services (destination ports) you may prohibit your LAN computers from using. Select the port you want to block, and click <b>Add</b> to add the port to the <b>Blocked Services</b> field.</p> <p>A custom port is a service that is not available in the pre-defined <b>Available Services</b> list. You must define it using the <b>Type</b> and <b>Port Number</b> fields. See <a href="#">Appendix E on page 359</a> for some examples of services.</p>
Blocked Services	This is a list of services (ports) that are inaccessible to computers on your LAN when service blocking is effective. To remove a service from this list, select the service, and click <b>Delete</b> .
Type	Select <b>TCP</b> , <b>UDP</b> or <b>TCP and UDP</b> , based on which one the custom port uses.
Port Number	Enter the range of port numbers that defines the service. For example, suppose you want to define the Gnutella service. Select <b>TCP</b> type and enter a port range of <b>6345-6349</b> .
Add	Click this to add the selected service in <b>Available Services</b> to the <b>Blocked Services</b> list. Note that the service is blocked immediately after clicking this.
Delete	Select a service in the <b>Blocked Services</b> , and click this to remove the service from the list.
Clear All	Click this to remove all the services in the <b>Blocked Services</b> list.

**Table 52** Security > Firewall > Services (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 12.4 Firewall Technical Reference

This section provides some technical background information about the topics covered in this chapter.

### 12.4.1 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via web configurator.
- 2 Think about access control before you connect to the network in any way.
- 3 Limit who can access your Device.
- 4 Don't enable any local service (such as Telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Keep the firewall in a secured (locked) room.

### 12.4.2 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.





## MAC Filter

### 13.1 Overview

This chapter discusses MAC address filtering.

You can configure the Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections.

#### 13.1.1 What You Need to Know

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

### 13.2 The MAC Filter Screen

Use the **MAC Filter** screen to allow wireless and LAN clients access to the Device. To change your Device's MAC filter settings, click **Security > MAC Filter**. The screen appears as shown.

**Figure 91** Security > MAC Filter

MAC Address Filter : ☐ Enable ☒ Disable

Set	Allow	MAC Address
1	<input type="checkbox"/>	00:24:21:7E:20:96
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
29	<input type="checkbox"/>	
30	<input type="checkbox"/>	
31	<input type="checkbox"/>	
32	<input type="checkbox"/>	

**Note :**  
Only devices listed here are granted access to the network.

Apply Cancel

The following table describes the labels in this menu.

**Table 53** Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select <b>Enable</b> to activate MAC address filtering.
Set	This is the index number of the MAC address.
Allow	Select <b>Allow</b> to permit access to the Device. MAC addresses not listed will be denied access to the Device.  If you clear this, the <b>MAC Address</b> field for this set clears.
MAC Address	Enter the MAC addresses of the wireless station and LAN devices that are allowed access to the Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## Parental Control

### 14.1 Overview

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the Device performs parental control on a specific user.

### 14.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security > Parental Control** to open the following screen.

**Figure 92** Security > Parental Control

General

Parental Control : ☐ Enable ☒ Disable (settings are invalid when disabled)

Add new PCP

#	Status	PCP Name	Home Network User (MAC)	Internet Access Schedule	Network Service	Website Blocked	Modify
1		PCP1	All	M T W T F S S 01:30-23:59	configured	None	

Apply Cancel

The following table describes the fields in this screen.

**Table 54** Parental Control > Parental Control

LABEL	DESCRIPTION
Parental Control	Select <b>Enable</b> to activate parental control.
Add new PCP	Click this if you want to configure a new parental control rule.
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not.  A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User (MAC)	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, <b>None</b> will be shown.

**Table 54** Parental Control > Parental Control (continued)

LABEL	DESCRIPTION
Website Block	This shows whether the website block is configured. If not, <b>None</b> will be shown.
Modify	Click the <b>Edit</b> icon to go to the screen where you can edit the rule. Click the <b>Delete</b> icon to delete an existing rule.
Add	Click <b>Add</b> to create a new schedule.
Apply	Click <b>Apply</b> to save your changes back to the Device.

## 14.2.1 Add/Edit a Parental Control Rule

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

**Figure 93** Add/Edit Parental Control Rule

The screenshot shows a window titled "Add new PCP" with a close button in the top right corner. The window is divided into several sections:

- General**: Contains a checkbox for "Active", a text field for "Parental Control Profile Name", and a dropdown menu for "Home Network User" currently set to "All".
- Internet Access Schedule**: Includes a "Day:" section with checkboxes for "Everyday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday", and "Sunday", all of which are checked. Below this is a "Time (Start - End):" section with a range from "00:00" to "24:00" and a slider. At the bottom of this section are two radio buttons: "No access" (selected) and "Authorized access".
- Network Service**: Contains a "Network Service Setting:" dropdown menu set to "Block" and the text "selected service(s)". Below this is an "Add new service" button.
- Blocked Site/URL Keyword**: Includes an "Add" button, a "Delete" button, and a large text area for entering keywords.

At the bottom right of the window are "Apply" and "Back" buttons.

The following table describes the fields in this screen.

**Table 55** Add/Edit Parental Control Rule

LABEL	DESCRIPTION
General	
Active	Select the checkbox to activate this parental control rule.

**Table 55** Add/Edit Parental Control Rule (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select <b>Custom</b> , enter the LAN user's MAC address. If you select <b>All</b> , the rule applies to all LAN users.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Device to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access.
Network Service	
Network Service Setting	<p>If you select <b>Block</b>, the Device prohibits the users from viewing the Web sites with the URLs listed below.</p> <p>If you select <b>Access</b>, the Device blocks access to all URLs except ones listed below.</p>
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the <b>Service Name</b> , <b>Protocol</b> , and <b>Name</b> of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	<p>Click the <b>Edit</b> icon to go to the screen where you can edit the rule.</p> <p>Click the <b>Delete</b> icon to delete an existing rule.</p>
Blocked Site/URL Keyword	Click <b>Add</b> to show a screen to enter the URL of web site or URL keyword to which the Device blocks access. Click <b>Delete</b> to remove it.
Apply	Click this button to save your settings back to the Device.
Back	Click this button to return to the previous screen without saving any changes.



# Certificates

## 15.1 Overview

The Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

### 15.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Device's CA-signed certificates ([Section 15.2 on page 213](#)).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Device. You can also export the certificates to a computer ([Section 15.3 on page 215](#)).

### 15.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

#### Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

#### Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

## **Certification Path**

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Device does not trust a certificate if any certificate on its path has expired or been revoked.

## **Certificate Directory Servers**

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

## **Advantages of Certificates**

Certificates offer the following benefits.

- The Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

## **Certificate File Formats**

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

**Note:** Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

### **15.1.3 Verifying a Certificate**

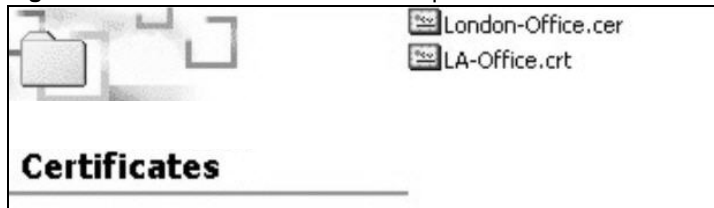
Before you import a trusted CA or trusted remote host certificate into the Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the Device also trusts any valid certificate signed by any of the imported trusted CA certificates.



You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

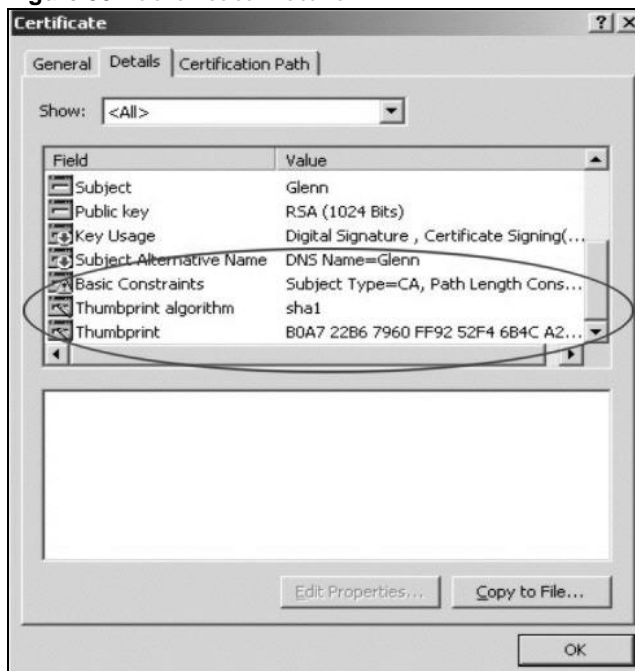
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 94** Certificates on Your Computer



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

**Figure 95** Certificate Details



- 4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

## 15.2 Local Certificates

Use this screen to view the Device's summary list of certificates and certification requests. You can import the following certificates to your Device:

- Web Server - This certificate secures HTTP connections.

- SIP TLS - This certificate secures VoIP connections.
- SSH/SCP/SFTP - This certificate secures remote connections.

Click **Security > Certificates** to open the **Local Certificates** screen.

**Figure 96** Security > Certificates > Local Certificates

Replace PrivateKey/Certificate file in PEM format

WebServer  [Browse...](#)

Current File	Subject	Issuer	Valid From	Valid To	Cert
web.pem	O=ZyXEL, CN=zyxel.com.tw	O=ZyXEL, CN=zyxel.com.tw	2009-10-07 00:48:07 GMT	2019-10-05 00:48:07 GMT	

SSH/SCP/SFTP  [Browse...](#)

Current File	Key Type
ssh.rsa	RSA

**Note :**  
SSH/SCP/SFTP -- Maximum key length supported is up to 4096 bits (default is 2048 bits), and the initialization time is proportional to key length. You need to adjust your application timeout settings to adapt this variation.

[Replace](#) [Reset](#)

The following table describes the labels in this screen.

**Table 56** Security > Certificates > Local Certificates

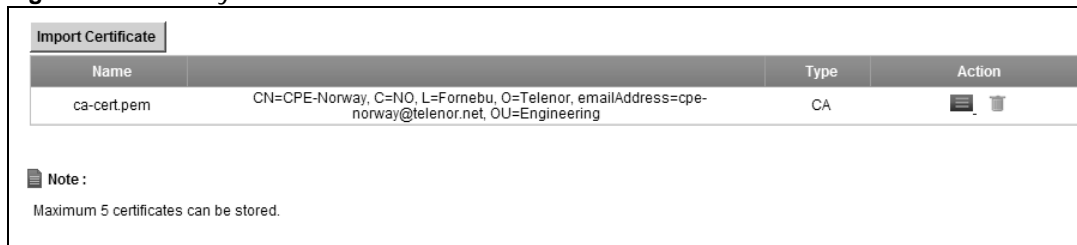
LABEL	DESCRIPTION
WebServer	Click <b>Browse...</b> to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as <b>CN</b> (Common Name), <b>OU</b> (Organizational Unit or department), <b>O</b> (Organization or company) and <b>C</b> (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a <b>Not Yet Valid!</b> message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an <b>Expiring!</b> or <b>Expired!</b> message if the certificate is about to expire or has already expired.
Cert	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
SSH/SCP/SFTP	Type in the location of the <b>SSH/SCP/SFTP</b> certificate file you want to upload in this field or click <b>Browse</b> to find it.
Choose file	Click this link to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Key Type	This field applies to the <b>SSH/SCP/SFTP</b> certificate.  This shows the file format of the current certificate.
Replace	Click this to replace the certificate(s) and save your changes back to the Device.
Reset	Click this to clear your settings.

## 15.3 Trusted CA

Use this screen to view a summary list of certificates of the certification authorities that you have set the Device to accept as trusted. The Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen.

**Figure 97** Security > Certificates > Trusted CA



The following table describes the labels in this screen.

**Table 57** Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Device.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. <b>ca</b> means that a Certification Authority signed the certificate.
Action	Click the <b>View</b> icon to open a screen with an in-depth list of information about the certificate (or certification request).  Click the <b>Delete</b> icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

## 15.4 Trusted CA Import

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the Device.

Note: You must remove any spaces from the certificate’s filename before you can import the certificate.

Figure 98 Trusted CA > Import

The certificate is in one of the following formats.  
Binary X.509  
PEM (Base-64) encoded  
Binary PKCS#7  
PEM (Base-64) encoded PKCS#7

Certificate File Path: 

Choose File

 No file chosen

Apply

Back

The following table describes the labels in this screen.

Table 58 Security > Certificates > Trusted CA > Import

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the Device.
Back	Click <b>Back</b> to return to the previous screen.

## 15.5 View Certificate

Use this screen to view in-depth information about the certification authority’s certificate, change the certificate’s name and set whether or not you want the Device to check a certification authority’s list of revoked certificates before trusting a certificate issued by the certification authority.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

**Figure 99** Trusted CA: View



The following table describes the labels in this screen.

**Table 59** Trusted CA: View

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate Detail	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Back	Click this to return to the previous screen.



## 16.1 Overview

Use this chapter to:

- Connect an analog phone to the Device.
- Make phone calls over the Internet, as well as the regular phone network.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

### 16.1.1 What You Can Do in this Chapter

These screens allow you to configure your Device to make phone calls over the Internet and your regular phone line, and to set up the phones you connect to the Device.

- Use the **SIP Service Provider** screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions ([Section 16.3 on page 224](#)).
- Use the **SIP Account** screen to set up information about your SIP account, control which SIP accounts the phones connected to the Device use and configure audio settings such as volume levels for the phones connected to the ZyXEL Device ([Section 16.3 on page 224](#)).
- Use the **Common** screen to configure RFC3262 support on the Device ([Section 16.5 on page 228](#)).
- Use the **Phone Device** screen to control which SIP accounts the phones connected to the Device use ([Section 16.6 on page 229](#)).
- Use the **Region** screen to change settings that depend on the country you are in ([Section 16.7 on page 231](#)).
- Use the **Call Rule** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers ([Section 16.8 on page 231](#)).
- Use the **FXO** screen to set up the PSTN line used to make regular phone calls which do not use the Internet ([Section 16.9 on page 233](#)).

You don't necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

### 16.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

## VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

## SIP

SIP stands for Session Initiation Protocol. SIP is a signalling standard that lets one network device (like a computer or the Device) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your Device, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call.

## SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the Device to use your SIP account to make calls, the Device is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you don't need a SIP account. It is possible for one SIP device (like the Device) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup - figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

## Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

## Comfort Noise Generation

When using VAD, the Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

## Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

Use this screen to maintain basic information about each SIP account. You can also enable and disable each SIP account, configure the volume, echo cancellation and VAD (Voice Activity Detection) settings for each individual phone port on the Device.

## How to Find Out More

See [Chapter 3 on page 33](#) for a tutorial showing how to set up these screens in an example scenario.



See [Section on page 232](#) for advanced technical information on SIP.

### 16.1.3 Before You Begin

- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the Device.

## 16.2 The SIP Service Provider Screen

Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions and dialing plan. Click **VoIP > SIP** to open the **SIP Service Provider** screen.

Note: Click **more...** to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click **hide more** to see and configure only the fields needed for this feature.

**Figure 100** VoIP > SIP > SIP Service Provider

**SIP Service Provider Selection**  
Service Provider Selection : ChangeMe Delete

**General**  
SIP Service Provider : ☒ Enable SIP Service Provider  
SIP Service Provider Name : ChangeMe  
SIP Local Port : 5060 (1025-65535)  
SIP Server Address : ChangeMe  
SIP Server Port : 5060 (1025-65535)  
REGISTER Server Address : ChangeMe  
REGISTER Server Port : 5060 (1025-65535)  
SIP Service Domain : ChangeMe
[hide more](#)

**RTP Port Range**  
Start Port : 50000 (1025-65535)  
End Port : 65535 (1025-65535)

**DTMF Mode**  
DTMF Mode : RFC 2833

**Transport Type**  
Transport Type : UDP

**FAX Option**  
☒ G711 Fax Passthrough ☐ T38 Fax Relay

**Outbound Proxy**  
☐ Enable  
Server Address :   
Server Port :  (1025-65535)

**QoS Tag**  
SIP TOS Priority Setting : 0 (0-255)  
RTP TOS Priority Setting : 0 (0-255)

**Timer Setting**  
Expiration Duration : 3600 (60-65535) second  
Register Re-send timer : 512 (180-65535) second  
Session Expires : 180 (100-3600) second  
Min-SE : 90 (90-1800) second

**Dialing Interval Selection**  
Dialing Interval Selection : 3 second

**PSTN Fail Over**  
☐ Fall back to PSTN when SIP is unregistered or SIP call fail

Apply Cancel

The following table describes the labels in this screen.

**Table 60** VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen. If you change this field, the screen automatically refreshes.
General	
SIP Service Provider	Select this if you want the Device to use this SIP provider. Clear it if you do not want the Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the <b>SIP Server Address</b> field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the <b>SIP Server Port</b> field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
RTP Port Range	
Start Port End Port	<p>Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.</p> <p>To enter one port number, enter the port number in the <b>Start Port</b> and <b>End Port</b> fields.</p> <p>To enter a range of ports,</p> <ul style="list-style-type: none"> <li>enter the port number at the beginning of the range in the <b>Start Port</b> field.</li> <li>enter the port number at the end of the range in the <b>End Port</b> field.</li> </ul>
DTMF Mode	<p>Control how the Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.</p> <p><b>RFC2833</b> - send the DTMF tones in RTP packets.</p> <p><b>PCM</b> - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones.</p> <p><b>SIP INFO</b> - send the DTMF tones in SIP messages.</p>
Transport Type	
Transport Type	Select the transport layer protocol <b>UDP</b> or <b>TCP</b> (usually UDP) used for SIP.
FAX Option	This field controls how the Device handles fax messages.
G711 Fax Passthrough	Select this if the Device should use G.711 to send fax messages. The peer devices must also use G.711.

**Table 60** VoIP > SIP > SIP Service Provider (continued)

LABEL	DESCRIPTION
T38 Fax Relay	Select this if the Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Outbound Proxy	
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
QoS Tag	
SIP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Device accepts.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
PSTN Fail Over ("L" models only)	Select this check box if you want to redirect the outgoing calls to the PSTN line (that do not use the Internet) when your SIP account is unregistered or SIP call has failed.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.







## 16.3 The SIP Account Screen

The Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your Device to connect to your VoIP service provider.

See [Section 16.3 on page 224](#) for how to map a SIP account to a phone port.

To access the following screen, click **VoIP > SIP > SIP Account**.

**Figure 101** VoIP > SIP > SIP Account

Add new SIP account					
#	Active	SIP Account	SIP Service Provider	Account No.	Modify
1		SIP 1	ChangeMe	ChangeMe	 
2		SIP 2	ChangeMe	ChangeMe	 

The following table describes the labels in this screen.

**Table 61** VoIP > SIP > SIP Account

LABEL	DESCRIPTION
#	This is the index number of the entry.
Active	This shows whether the SIP account is activated or not.  A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is activated.
SIP Account	This shows the name of the SIP account.
SIP Service Provider	This shows the name of the SIP service provider.
Account No.	This shows the SIP number.
Modify	Click the <b>Edit</b> icon to configure the SIP account.  Click the <b>Delete</b> icon to delete this SIP account from the Device.

### 16.3.1 Add/Edit SIP Account

You can configure a new SIP account or edit one. To access this screen, click **Add new SIP Account** in the **SIP Account** screen or **Edit** icon next to an existing account.

**Figure 102** SIP Account: Add/Edit

SIP Service Provider Selection

Service Provider Selection : 

ChangeMe

General

SIP Account : 

☐ Active SIP Account

SIP Account Number : 

ChangeMe

Authenticaton

Username : 

ChangeMe

Password : 

.....

URL Type

URL Type : 

SIP

Voice Features

Primary Compression Type : 

G.711MuLaw

Second Compression Type : 

G.729

Third Compression Type : 

G.711ALaw

Speaking Volume Control : 

Middle

Listening Volume Control : 

Middle

☒ Active G.168(Echo Cancellation)

☒ Active VAD(Voice Active Detector)

Note :

VAD will not be active while G.722 is used.

Call Features

☒ Send Caller ID

☒ Active Call Transfer

☒ Active Call Waiting :

Active Call Waiting Reject Time : 

24

 (10-60) second

☐ Active Unconditional Forward

To Number :

☐ Active Busy Forward

To Number :

☐ Active No Answer Forward

To Number :

No Answer Ring Time 

10

 (10~180) Second

Apply

Back

Each field is described in the following table.

**Table 62** SIP Account: Edit

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen.  This field is view-only if you are editing the SIP account.
SIP Account Selection	
SIP Account Selection	This shows the SIP account you are configuring.
General	

**Table 62** SIP Account: Edit (continued)

LABEL	DESCRIPTION
SIP Account	Select the <b>Active SIP Account</b> check box if you want to use this account. Clear it if you do not want to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the Device sends the SIP number.  <b>SIP</b> - include the SIP service domain name. <b>TEL</b> - do not include the SIP service domain name.
Voice Features	
Primary Compression Type	Select the type of voice coder/decoder (codec) that you want the Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps).
Secondary Compression Type	<ul style="list-style-type: none"> <li>• <b>G.711MuLaw</b> is typically used in North America and Japan.</li> <li>• <b>G.711ALaw</b> is typically used in Europe.</li> <li>• <b>G.729</b> only requires 8 kbps.</li> <li>• <b>G.726-32</b> operates at 16, 24, 32 or 40 kbps.</li> <li>• <b>G.722</b> operates at 48, 56 and 64 kbps. The Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.</li> </ul>
Third Compression Type	<p>Select the Device's first choice for voice coder/decoder.</p> <p>Select the Device's second choice for voice coder/decoder. Select <b>None</b> if you only want the Device to accept the first choice.</p> <p>Select the Device's third choice for voice coder/decoder. Select <b>None</b> if you only want the Device to accept the first or second choice.</p>
Speaking Volume Control	Enter the loudness that the Device uses for speech that it sends to the peer device.  <b>Minimum</b> is the quietest, and <b>Maximum</b> is the loudest.
Listening Volume Control	Enter the loudness that the Device uses for speech that it receives from the peer device.  <b>Minimum</b> is the quietest, and <b>Maximum</b> is the loudest.
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD (Voice Active Detector)	Select this if the Device should stop transmitting when you are not speaking. This reduces the bandwidth the Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Active Call Transfer	Select this to enable call transfer on the Device. This allows you to transfer an incoming call (that you have answered) to another phone.

**Table 62** SIP Account: Edit (continued)

LABEL	DESCRIPTION
Active Call Waiting	Select this to enable call waiting on the Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Active Call Waiting Reject Time	Specify a time of seconds that the Device waits before rejecting the second call if you do not answer it.
Active Unconditional Forward	Select this if you want the Device to forward all incoming calls to the specified phone number. Specify the phone number in the <b>To Number</b> field on the right.
Active Busy Forward	Select this if you want the Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the <b>To Number</b> field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Active No Answer Forward	Select this if you want the Device to forward incoming calls to the specified phone number if the call is unanswered. (See <b>No Answer Time</b> .) Specify the phone number in the <b>To Number</b> field on the right.
No Answer Ring Time	This field is used by the <b>Active No Answer Forward</b> feature. Enter the number of seconds the Device should wait for you to answer an incoming call before it considers the call is unanswered.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen without saving.

## 16.4 Multiple SIP Accounts

You can set up two SIP accounts on your Device and your Device is equipped with two phone ports. By default, SIP1 of the Device maps to phone port 1 for incoming and outgoing, and SIP2 maps to phone port 2 for incoming and outgoing.

## 16.5 The Common Screen

Use the **Common** screen to configure RFC3262 support on the Device. To access the following screen, click **VoIP > SIP > Common**.

**Figure 103** VoIP > SIP > Common

**Bound Interface Name**  
Bound Interface Name : AnyWAN

**RFC Support**  
PRACK (RFC 3262): Supported

☒ Session Timer (RFC 4028)

Apply Cancel



Each field is described in the following table.



**Table 63** VoIP > SIP > Common

LABEL	DESCRIPTION
Bound Interface Name	
Bound Interface Name	<p>If you select <b>AnyWAN</b>, the Device automatically activates the VoIP service when any WAN connection is up.</p> <p>If you select <b>MultiWAN</b>, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.</p>
RFC Support	
PRACK (RFC 3262)	<p>RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method.</p> <p>Select <b>Supported</b> or <b>Required</b> to have the Device include a SIP Require/Supported header field with the option tag 100rel in all INVITE requests. When the Device receives a SIP response message indicating that the phone it called is ringing, the Device sends a PRACK message to have both sides confirm the message is received.</p> <p>If you select <b>Supported</b>, the peer device supports the option tag 100rel to send provisional responses reliably.</p> <p>If you select <b>Required</b>, the peer device requires the option tag 100rel to send provisional responses reliably.</p> <p>Select <b>Disabled</b> to turn off this function.</p>
Session Timer (RFC 4028)	<p>Select this to have the Device support RFC 4028.</p> <p>This makes sure that SIP sessions do not hang and the SIP line can always be available for use.</p>
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to return to the previous screen without saving.

## 16.6 Phone Screen

Use this screen to control which SIP accounts and PSTN line each phone uses. Click **VoIP > Phone** to access the **Phone Device** screen.

**Figure 104** VoIP > Phone > Phone Device

Analog Phone			
#	Phone ID	Outgoing SIP Number	Modify
1	Analog Phone 1	ChangeMe	
2	Analog Phone 2	ChangeMe	

The following table describes the labels in this screen.

**Table 64** VoIP > Phone > Phone Device

LABEL	DESCRIPTION
#	This is the index number of the entry.
Phone ID	This is the phone device number.
Outgoing SIP Number	This is the outgoing SIP number of the phone device.
Modify	Click the <b>Edit</b> icon to configure the SIP account.

## 16.6.1 Edit Phone Device

You can decide which SIP accounts the phones connected to the Device use by clicking the **Edit** icon next to a Phone ID. The following screen displays.

You cannot edit the account if it is not activated. Go to **VoIP > SIP > SIP Account > Edit** to activate a SIP account (see [Section 16.3 on page 224](#) for more information).

**Figure 105** Phone Device: Edit

**SIP Account to Make Outgoing Call**

SIP Account	SIP Number	SIP Account	SIP Number
<input checked="" type="radio"/> SIP 1	ChangeMe	<input type="radio"/> SIP 2	ChangeMe

**SIP Account(s) to Receive Incoming Call**

SIP Account	SIP Number	SIP Account	SIP Number
<input checked="" type="checkbox"/> SIP 1	ChangeMe	<input type="checkbox"/> SIP 2	ChangeMe

**FXO Interface to Receive Incoming Call**

☒ Enable

Apply Back

The following table describes the labels in this screen.

**Table 65** Phone Device: Edit

LABEL	DESCRIPTION
SIP Account to Make Outgoing Call	
SIP Account	Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.
SIP Number	This shows the SIP account number.
SIP Account(s) to Receive Incoming Call	
SIP Account	Select a SIP account if you want to receive phone calls for the selected SIP account on this phone port.  If you select more than one SIP account for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port.
SIP Number	This shows the SIP account number.

**Table 65** Phone Device: Edit (continued)

LABEL	DESCRIPTION
FXO Interface to Receive Incoming Call	
Enable	Select this if you want to receive phone calls from the PSTN line (that do not use the Internet) on this phone port.
Apply	Click <b>Apply</b> to save your changes.
Back	Click <b>Back</b> to return to the previous screen without saving.

## 16.7 The Phone Region Screen

Use this screen to maintain settings that depend on which region of the world the Device is in. To access this screen, click **VoIP > Phone > Region**.

**Figure 106** VoIP > Phone > Region

Region Settings : USA

Call Service Mode : Europe Type

**Note :**

Caution: When Region Settings is changed, you need to reboot device to take settings effect.

Apply Cancel

Each field is described in the following table.

**Table 66** VoIP > Phone > Region

LABEL	DESCRIPTION
Region Settings	Select the place in which the Device is located.
Call Service Mode	<p>Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports.</p> <ul style="list-style-type: none"> <li><b>Europe Type</b> - use supplementary phone services in European mode.</li> <li><b>USA Type</b> - use supplementary phone services American mode.</li> </ul> <p>You might have to subscribe to these services to use them. Contact your VoIP service provider.</p>
Apply	Click this to save your changes and to apply them to the Device.
Cancel	Click this to set every field in this screen to its last-saved value.

## 16.8 The Call Rule Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

To access this screen, click **VoIP > Call Rule**.

**Figure 107** VoIP > Call Rule

**Speed Dial**

#	Number	Description	SIPNumber
1			<div>Add</div>

**Phone Book**

#	Number	Description	Modify
#01			<div><div></div><div></div></div>
#02			<div><div></div><div></div></div>
#03			<div><div></div><div></div></div>
#04			<div><div></div><div></div></div>
#05			<div><div></div><div></div></div>
#06			<div><div></div><div></div></div>
#07			<div><div></div><div></div></div>
#08			<div><div></div><div></div></div>
#09			<div><div></div><div></div></div>
#10			<div><div></div><div></div></div>

Clear

Cancel

Each field is described in the following table.

**Table 67** VoIP > Call Rule

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Add	Click this to use the information in the <b>Speed Dial</b> section to update the <b>Speed Dial Phone Book</b> section.
Phone Book	Use this section to look at all the speed-dial entries and to erase them.
#	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the Device calls when you dial the speed-dial number.
Description	This field displays a short description of the party you call when you dial the speed-dial number.
Modify	<div>Use this field to edit or erase the speed-dial entry.</div> <div>Click the <b>Edit</b> icon to copy the information for this speed-dial entry into the <b>Speed Dial</b> section, where you can change it. Click <b>Add</b> when you finish editing to change the configurations.</div> <div>Click the <b>Delete</b> icon to erase this speed-dial entry.</div>
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

## 16.9 The FXO Screen (“L” Models Only)

With PSTN line you can make and receive regular PSTN phone calls. Use a prefix number to make a regular call. When the device does not have power, you can make regular calls without dialing a prefix number.

**When the Device does not have power, only the phone connected to the PHONE port1 can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.**

Use the **FXO** screen to set up the PSTN line you use to make regular phone calls which do not use the Internet. To access this screen, click **VoIP > FXO**.

**Figure 108** VoIP > FXO

Each field is described in the following table.

**Table 68** VoIP > FXO

LABEL	DESCRIPTION
Pre-Fix For FXO Outgoing Call	
Pre-Fix Number	Enter 1 - 7 numbers you dial before you dial the phone number, if you want to make a regular phone call while one of your SIP accounts is registered. These numbers tell the Device that you want to make a regular phone call.
Voice Features	
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD (Voice Active Detector)	Select this if the Device should stop transmitting when you are not speaking. This reduces the bandwidth the Device uses.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 16.10 Technical Reference

This section contains background material relevant to the **VoIP** screens.

## 16.10.1 VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

## 16.10.2 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

### SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

### SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

### SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is [1122334455@VoIP-provider.com](mailto:1122334455@VoIP-provider.com), then "VoIP-provider.com" is the SIP service domain.

### SIP Registration

Each Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the Device attempts to register the port immediately.

## Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC3261, "SIP: Session Initiation Protocol").

## SIP Servers

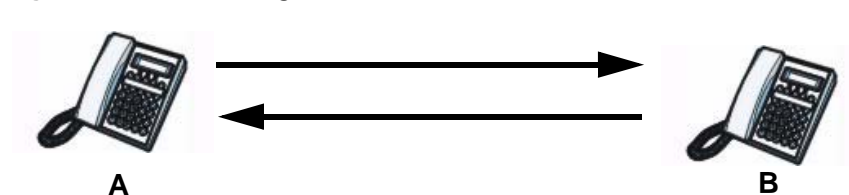
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

## SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

**Figure 109** SIP User Agent



## SIP Proxy Server

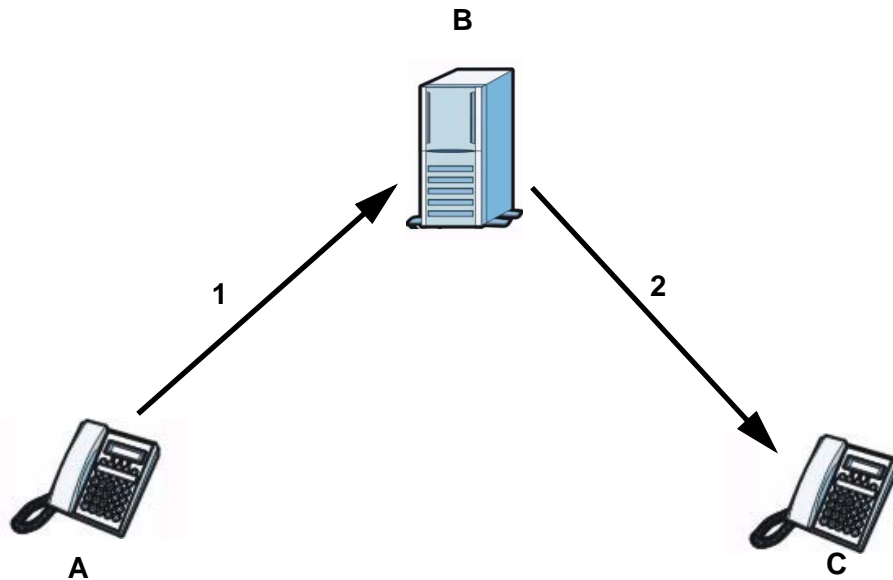
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device **C**.

- 1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server **B**.

- 2 The SIP proxy server forwards the call invitation to **C**.

**Figure 110** SIP Proxy Server



### SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

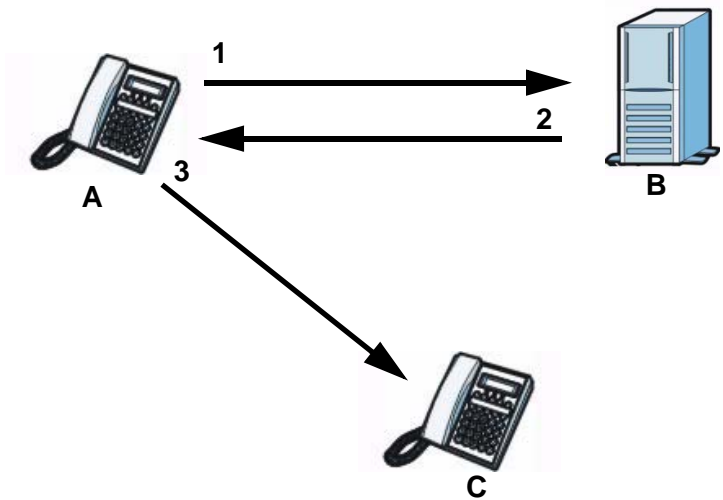
In the following example, you want to use client device **A** to call someone who is using client device **C**.

- 1 Client device **A** sends a call invitation for **C** to the SIP redirect server **B**.
- 2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).



- 3 Client device **A** then sends the call invitation to client device **C**.

**Figure 111** SIP Redirect Server



**SIP Register Server**

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

**RTP**

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 3550 for details on RTP.

**Pulse Code Modulation**

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

**SIP Call Progression**

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

**Table 69** SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	
	5. Dialogue (voice traffic)	
6. BYE	→	
	←	7. OK

- 1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.
- 2 **B** sends a response indicating that the telephone is ringing.
- 3 **B** sends an OK response after the call is answered.
- 4 **A** then sends an ACK message to acknowledge that **B** has answered the call.
- 5 Now **A** and **B** exchange voice media (talk).
- 6 After talking, **A** hangs up and sends a BYE request.
- 7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

## Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

## PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.<sup>3</sup>

## MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

### 16.10.3 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

---

3. The Device does not support pulse dialing at the time of writing.

## Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

## DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.<sup>4</sup>

## DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

**Figure 112** DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)
-----------------	-------------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

## VLAN Tagging

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

## 16.10.4 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer, are generally available from your VoIP service provider. The Device supports the following services:

4. The Device does not support DiffServ at the time of writing.

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Three-Way Conference
- Internal Calls
- Do not Disturb

Note: To take full advantage of the supplementary phone services available through the Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

## The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the Device.

You can invoke all the supplementary services by using the flash key.

## Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command time-out (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

**Table 70** European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

## European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

## European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.  
Press the flash key and then press "0".
- Disconnect the first call and answer the second call.  
Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.  
Press the flash key and then "2".

## European Call Transfer

Do the following to transfer a call (that you have answered) to another phone number.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial "\*98#" followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

## European Three-Way Conference

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone, press the flash key to put the call on hold and get a dial tone.
- 2 Dial a phone number directly to make another call.

- 3 When the second call is answered, press the flash key and press "3" to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".

## 17.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the Device log and then display the logs or have the Device send them to an administrator (as e-mail) or to a syslog server.

### 17.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs for the categories that you select ([Section 17.2 on page 244](#)).
- Use the **Phone Log** screen to view phone logs and alert messages ([Section 17.3 on page 245](#)).
- Use The **VoIP Call History** screen to view the details of the calls performed on the Device ([Section 17.4 on page 245](#)).

### 17.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

#### Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

#### Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

**Table 71** Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.

**Table 71** Syslog Severity Levels

CODE	SEVERITY
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

## 17.2 The System Log Screen

Click **System Monitor > Log** to open the **System Log** screen. Use the **System Log** screen to see the system logs for the categories that you select in the upper left drop-down list box.

**Figure 113** System Monitor > Log > System Log

Remote Management Level: All Refresh Clear Logs			
#	Time	Level	Message
1	1970 Jan 13 08:35:32	notice	Send DHCP ACK to 00:24:21:7E:20:96 with IP 192.168.
2	1970 Jan 13 08:35:32	notice	Receive DHCP REQUEST from 00:24:21:7E:2
3	1970 Jan 13 08:35:27	notice	Send DHCP ACK to 00:24:21:7E:20:96 with IP 192.168.
4	1970 Jan 13 08:35:27	notice	Receive DHCP REQUEST from 00:24:21:7E:2
5	1970 Jan 13 08:35:27	notice	Send DHCP OFFER to 00:24:21:7E:20:96 with IP 192.168.
6	1970 Jan 13 08:35:27	notice	Receive DHCP DISCOVER from 00:24:21:7E:2
7	1970 Jan 13 08:35:22	notice	Send DHCP NACK to 00:24:21:7E:2
8	1970 Jan 13 08:35:22	notice	Receive DHCP REQUEST from 00:24:21:7E:2

The following table describes the fields in this screen.

**Table 72** System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Device searches through all logs of that severity or higher.
Refresh	Click this to renew the log screen.
Clear Log	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.



## 17.3 The Phone Log Screen

Click **System Monitor > Log** to open the **Phone Log** screen. Use this screen to view phone logs and alert messages. You can select the type of log and level of severity to display.

**Figure 114** System Monitor > Log > Phone Log

AllLogs	Level: All	Refresh	Clear Logs
#	Time	Level	Message
1	Aug 20 07:37:17	err	SIP Registration: SIP:12875: Register Fail, error_cause 43
2	Aug 20 07:37:40	info	[ChangeMe] [FXS2] Phone Event: OFFHOOK
3	Aug 20 07:37:43	info	[ChangeMe] [FXS2] Phone Event: ONHOOK
4	Aug 20 07:37:43	info	[ChangeMe] [FXS2] Phone Event: idle
5	Aug 20 07:39:05	info	[ChangeMe] [FXS2] Phone Event: OFFHOOK
6	Aug 20 07:39:28	info	[ChangeMe] [FXS2] Phone Event: ONHOOK
7	Aug 20 07:39:28	info	[ChangeMe] [FXS2] Phone Event: idle
8	Aug 20 07:41:14	info	SIP Registration: SIP:128752: Register Success
9	Aug 20 07:41:49	info	[ChangeMe] [FXS2] Phone Event: OFFHOOK
10	Aug 20 07:41:56	info	[ChangeMe] [FXS2] Phone Event: ONHOOK

The following table describes the fields in this screen.

**Table 73** System Monitor > Log > Phone Log

LABEL	DESCRIPTION
	Select a category of logs to view from the drop-down list box. select <b>All Logs</b> to view all logs.
Level	Select the severity level that you want to view.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Message	This field states the reason for the log.

## 17.4 The VoIP Call History Screen

Click **System Monitor > Log > VoIP Call History** to open the **VoIP Call History** screen. Use this screen to see the details of the calls performed on the Device.

**Figure 115** System Monitor > Log > VoIP Call History

All Call History

Refresh

Clear Logs

#	Time	Local Number	Peer Number	Interface	Duration
1	08/20/2010 09:43:52	128752	1353699	SIP	0:00:00
2	08/20/2010 09:43:07	128752	1353699	SIP	0:00:06
3	08/20/2010 09:42:11	128752	1353699	SIP	0:00:37

The following table describes the fields in this screen.

**Table 74** System Monitor > Log > VoIP Call History

LABEL	DESCRIPTION
	Select a category of call records to view from the drop-down list box. select <b>All Call History</b> to view all call records.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the call was recorded.
Local Number	This field displays the phone number you used to make or receive this call.
Peer Number	This field displays the phone number you called or from which this call is made.
Interface	This field displays the type of the call.
Duration	This field displays how long the call lasted.

# Traffic Status

## 18.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

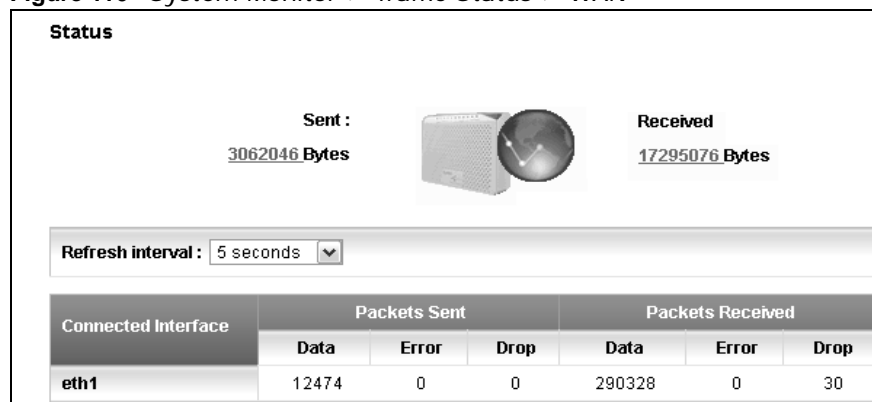
### 18.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 18.2 on page 247](#)) .
- Use the **LAN** screen to view the LAN traffic statistics ([Section 18.3 on page 248](#)).
- Use the **NAT** screen to view the NAT status of the Device's client(s) ([Section 18.4 on page 249](#)).
- Use the **3G Backup** screen to view the 3G connection traffic statistics ([Section 18.6 on page 251](#)).
- Use the **VoIP Status** screen to view the VoIP traffic statistics ([Section 18.6 on page 251](#)).

## 18.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. You can view the WAN traffic statistics in this screen.

**Figure 116** System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

**Table 75** System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes received and sent through the WAN interface of the Device.
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

## 18.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. You can view the LAN traffic statistics in this screen.

**Figure 117** System Monitor > Traffic Status > LAN

Refresh interval : 5 seconds ▼

Interface	LAN1	LAN2	LAN3	LAN4	Wireless
Bytes Sent	8027614	0	0	0	2772
Bytes Received	1159174	0	0	0	3322

Interface	LAN1	LAN2	LAN3	LAN4	Wireless
Sent (Packet)	Data	11290	0	0	28
	Error	0	0	0	9
	Drop	0	0	0	0
Received (Packet)	Data	9452	0	0	27
	Error	0	0	0	0
	Drop	0	0	0	0

The following table describes the fields in this screen.

**Table 76** System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Interface	This shows the LAN or WLAN interface.

**Table 76** System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interface.
Sent (Packet)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packet)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

## 18.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. You can view the NAT status of the Device's client(s) in this screen.

**Figure 118** System Monitor > Traffic Status > NAT

Refresh interval : 5 seconds ▾			
Device Name	IP Address	MAC Address	No. of Open Session
twpc13774-02	192.168.1.58	00:24:21:7e:20:96	142
			Total : 142

The following table describes the fields in this screen.

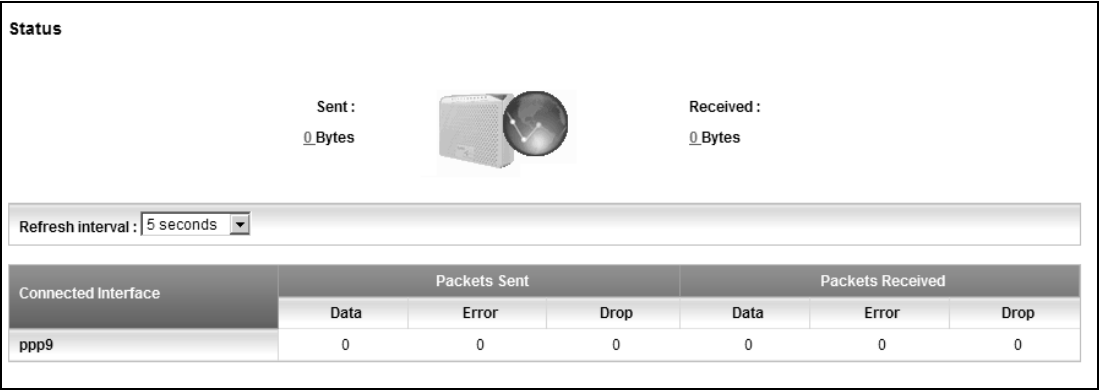
**Table 77** System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Device Name	This shows the name of the client.
IP Address	This shows the IP address of the client.
MAC Address	This shows the MAC address of the client.
No. of Open Session	This shows the number of NAT sessions used by the client.

# 18.5 The 3G Backup Status Screen

Click **System Monitor > Traffic Status > 3G Backup** to open the following screen. You can view the 3G connection traffic statistics in this screen.

**Figure 119** System Monitor > Traffic Status > 3G Backup



The following table describes the fields in this screen.

**Table 78** System Monitor > Traffic Status > 3G backup

LABEL	DESCRIPTION
Status	This shows the number of bytes received and sent through the 3G interface of the Device.
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
Connected Interface	This shows the name of the 3G connection interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

## 18.6 The VoIP Status Screen

Click **System Monitor > VoIP Status** to open the following screen. You can view the VoIP traffic statistics in this screen.

**Figure 120** System Monitor > VoIP Status

Refresh interval : 5 seconds

SIP Status

Account	Registration	Last Registration	URI	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP 1	Disabled	0:00:00	ChangeMe@ChangeMe	NO	N/A	N/A
SIP 2	Disabled	0:00:00	ChangeMe@ChangeMe	NO	N/A	N/A

Call Status

Account	Duration	Status	Codec	Peer Number
SIP 1	0 Day(s), 0 Hour(s), 0 Minute(s), 0 Second(s)	Idle		None
SIP 2	0 Day(s), 0 Hour(s), 0 Minute(s), 0 Second(s)	Idle		None

Phone Status

Account	Outgoing Number	Incoming Number	Phone State
Phone 1	ChangeMe	ChangeMe	ONHOOK
Phone 2	ChangeMe	ChangeMe	ONHOOK

The following table describes the fields in this screen.

**Table 79** System Monitor > VoIP Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen from the drop-down list box.
<b>SIP Status</b>	
Account	This column displays each SIP account in the Device.
Registration	<p>This field displays the current registration status of the SIP account. You can change this in the <b>Status</b> screen.</p> <p><b>Registered</b> - The SIP account is registered with a SIP server.</p> <p><b>Not Registered</b> - The last time the Device tried to register the SIP account with the SIP server, the attempt failed. The Device automatically tries to register the SIP account when you turn on the Device or when you activate it.</p> <p><b>Inactive</b> - The SIP account is not active. You can activate it in <b>VoIP &gt; SIP &gt; SIP Account</b>.</p>
Last Registration	This field displays the last time you successfully registered the SIP account. The field is blank if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the <b>VoIP &gt; SIP</b> screens.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
<b>Call Status</b>	
Account	This column displays each SIP account in the Device.

**Table 79** System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Duration	This field displays how long the current call has lasted.
Status	<p>This field displays the current state of the phone call.</p> <p><b>Idle</b> - There are no current VoIP calls, incoming calls or outgoing calls being made.</p> <p><b>Dial</b> - The callee's phone is ringing.</p> <p><b>Ring</b> - The phone is ringing for an incoming VoIP call.</p> <p><b>Process</b> - There is a VoIP call in progress.</p> <p><b>DISC</b> - The callee's line is busy, the callee hung up or your phone was left off the hook.</p>
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Account	This field displays the phone accounts of the Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Phone State	This field shows whether or the phone connected to the subscriber port is on-hook ( <b>ONHOOK</b> ) or off-hook ( <b>OFFHOOK</b> ).



## User Account

### 19.1 Overview

You can configure system password for different user accounts in the **User Account** screen.

### 19.2 The User Account Screen

Use the **User Account** screen to configure system password.

Click **Maintenance > User Account** to open the following screen.

**Figure 121** Maintenance > User Account

The screenshot shows a web-based configuration interface for user accounts. It contains the following elements:

- User Name :** A dropdown menu with 'admin' selected.
- Old Password :** A text input field.
- New Password :** A text input field.
- Retype to Confirm :** A text input field.
- Buttons:** 'Apply' and 'Cancel' buttons located at the bottom right of the form.

The following table describes the labels in this screen.

**Table 80** Maintenance > User Account

LABEL	DESCRIPTION
User Name	You can configure the password for the <b>Power User</b> and <b>Admin</b> accounts.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.



## Remote MGMT

### 20.1 Overview

**Remote MGMT** allows you to manage your Device from a remote location through the following interfaces:

- LAN and WLAN
- WAN only

Note: The Device is managed using the web configurator.

#### 20.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter

##### TR-064

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

##### SSH/SCP/SFTP

Secure Shell (SSH) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. The following file transfer methods use SSH:

- **Secure Copy (SC)** is a secure way of transferring files between computers. It uses port 22.
- **SSH File Transfer Protocol or Secure File Transfer Protocol (SFTP)** is an old way of transferring files between computers. It uses port 22.

## 20.2 The Remote MGMT Screen

Use this screen to decide what services you may use to access which Device interface. Click **Maintenance > Remote MGMT** to open the following screen.

**Figure 122** Maintenance > Remote MGMT

Remote Management

Services	LAN/WLAN	WAN	Port
HTTPS	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	443
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
TELNET	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
SSH/SCP/SFTP	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
ICMP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	N/A
TR-064	<input checked="" type="checkbox"/> Enable	N/A	18888

Apply

Cancel

The following table describes the fields in this screen.

**Table 81** Maintenance > Remote MGMT

LABEL	DESCRIPTION
Services	This is the service you may use to access the Device.
LAN/WLAN	Select the <b>Enable</b> check box for the corresponding services that you want to allow access to the Device from the LAN and WLAN.
WAN	Select the <b>Enable</b> check box for the corresponding services that you want to allow access to the Device from the WAN.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

# System

## 21.1 Overview

You can configure system settings, including the host name, domain name and the inactivity time-out interval in the **System** screen.

### 21.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter.

#### Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address "www.zyxel.com/support/files", the domain name is "www.zyxel.com".

## 21.2 The System Screen

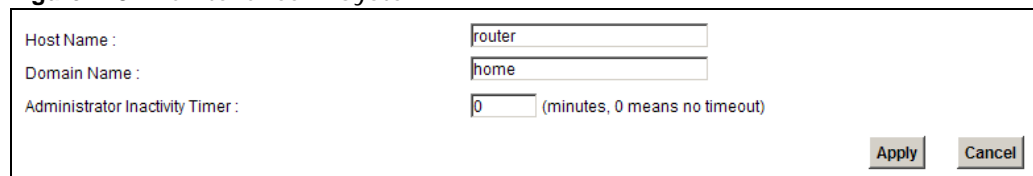
Use the **System** screen to configure the system's host name, domain name, and inactivity time-out interval.

The **Host Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer.

In Windows XP, click **start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Device **System Name**.

Click **Maintenance > System** to open the following screen.

**Figure 123** Maintenance > System



Host Name :	<input type="text" value="router"/>
Domain Name :	<input type="text" value="home"/>
Administrator Inactivity Timer :	<input type="text" value="0"/> (minutes, 0 means no timeout)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

**Table 82** Maintenance > System

<b>LABEL</b>	<b>DESCRIPTION</b>
Host Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.  The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click this to save your changes back to the Device.
Cancel	Click this to begin configuring this screen afresh.

## Time Setting

### 22.1 Overview

You can configure the system's time and date in the **Time Setting** screen.

### 22.2 The Time Setting Screen

To change your Device's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the Device's time based on your local time zone.

**Figure 124** Maintenance > Time Setting

The screenshot shows the 'Time Setting' screen with the following fields and options:

- Current Date/Time**
  - Current Time : 03:34:19
  - Current Date : 2000-01-01
- Time and Date Setup**
  - Time Protocol : NTP
  - Time Server Address : europe.pool.ntp.org
- Time Zone**
  - Time Zone : (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna
  - ☒ Daylight Savings
  - Start Date : Last Sun. Of March (2000-03-26) at 1 o'clock
  - End Date : Last Sun. Of October (2000-10-29) at 1 o'clock

Buttons: Apply, Reset

The following table describes the fields in this screen.

**Table 83** Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your Device.
Current Date	This field displays the date of your Device.
Time and Date Setup	
Time Protocol	This shows the time service protocol that your time server sends when you turn on the Device.
Time Server Address	Enter the IP address or URL (up to 31 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

**Table 83** Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Daylight Savings</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Second, Sunday, March</b> and type <b>2</b> in the <b>o'clock</b> field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type <b>2</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, November</b> and type <b>2</b> in the <b>o'clock</b> field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type <b>2</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



## Log Setting

### 23.1 Overview

You can configure where the Device sends logs and which logs and/or immediate alerts the Device records in the **Log Setting** screen.

### 23.2 The Log Setting Screen

To change your Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

**Figure 125** Maintenance > Log Setting

**Syslog Setting**

Syslog Logging : ☐ Enable ☒ Disable

Syslog Server :  (IP Address)

UDP Port :  (Server Port)

**Active Log and Select Level**

Log Category	Log Level
<b>VoIP</b>	
<input type="checkbox"/> VoIP-Call Statistics	ALL
<input checked="" type="checkbox"/> VoIP-SIP Call Signaling	ALL
<input checked="" type="checkbox"/> VoIP-SIP Registrations	ALL
<input type="checkbox"/> VoIP-Phone Event	ALL
<input type="checkbox"/> VoIP-Misc	ALL
<b>System</b>	
<input type="checkbox"/> WAN-DHCP	ALL
<input type="checkbox"/> xDSL	ALL
<input type="checkbox"/> ETHER	ALL
<input type="checkbox"/> System Maintenance	ALL
<input type="checkbox"/> Remote Management	ALL
<input type="checkbox"/> TR-069	ALL
<input type="checkbox"/> NTP	ALL
<input type="checkbox"/> DDNS	ALL
<input type="checkbox"/> NAT	ALL
<input type="checkbox"/> Attack	ALL

Apply Cancel

The following table describes the fields in this screen.

**Table 84** Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The Device sends a log to an external syslog server. Select the <b>Enable</b> check box to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
Active Log and Select Level	
Log Category	Select the categories of logs that you want to record.
Log Level	Select the severity level of logs that you want to record. If you want to record all logs, select <b>ALL</b> .
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## Firmware Upgrade

### 24.1 Overview

This chapter explains how to upload new firmware to your Device. You can download new firmware releases from your nearest ZyXEL FTP site (or [www.zyxel.com](http://www.zyxel.com)) to use to upgrade your device's performance.

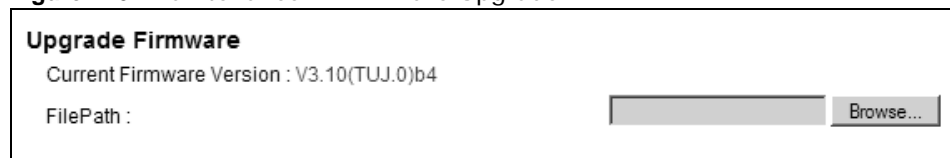
**Only use firmware for your device's specific model. Refer to the label on the bottom of your Device.**

### 24.2 The Firmware Upgrade Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the system will reboot.

**Do NOT turn off the Device while firmware upload is in progress!**

**Figure 126** Maintenance > Firmware Upgrade



**Upgrade Firmware**  
 Current Firmware Version : V3.10(TUJ.0)b4  
 FilePath :

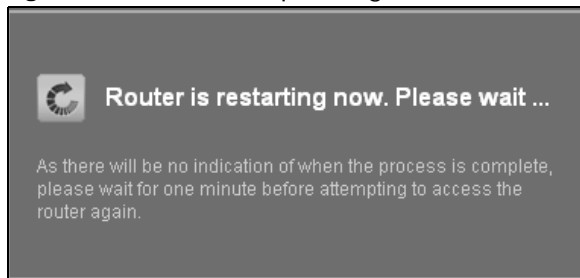
The following table describes the labels in this screen.

**Table 85** Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version.
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to three minutes.

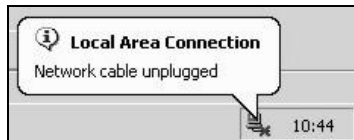
After you see the firmware updating screen, wait a few minutes before logging into the Device again.

**Figure 127** Firmware Uploading



The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

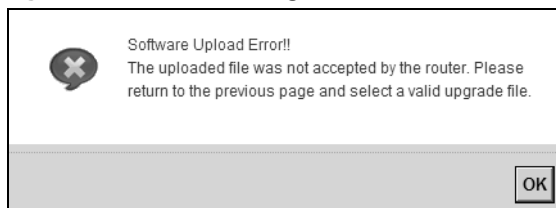
**Figure 128** Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

**Figure 129** Error Message



## Backup/Restore

### 25.1 Overview

The **Backup/Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

### 25.2 The Backup/Restore Screen

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

**Figure 130** Maintenance > Backup/Restore

**Backup Configuration**  
Click Backup to save the current configuration of your system to your computer.

**Restore Configuration**  
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.  
FilePath :

**Back to Factory Defaults**  
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the LAN IP address will be 192.168.1.1 DHCP will be reset to server

#### Backup Configuration

Backup Configuration allows you to back up (save) the Device's current configuration to a file on your computer. Once your Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Device's current configuration to your computer.

## Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Device.

**Table 86** Restore Configuration

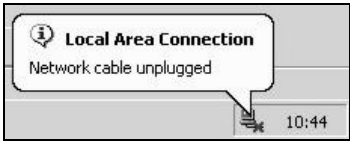
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your device settings back to the factory default.

**Do not turn off the Device while configuration file upload is in progress.**

After the Device configuration has been restored successfully, the login screen appears. Login again to restart the Device.

The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 131** Network Temporarily Disconnected



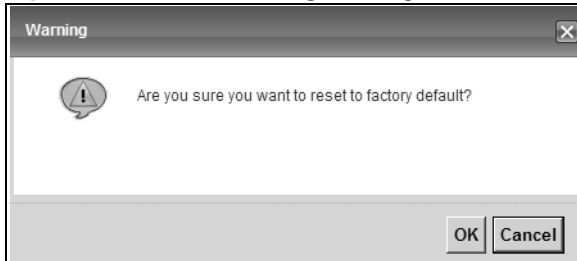
If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See [Appendix B on page 299](#) for details on how to set up your computer's IP address.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

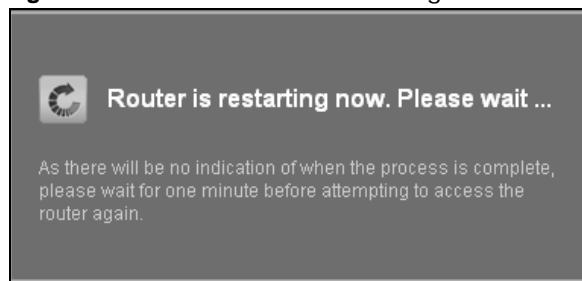
## Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Device to its factory defaults. The following warning screen appears.

**Figure 132** Reset Warning Message



**Figure 133** Reset In Process Message



You can also press the **RESET** button on the back panel to reset the factory defaults of your Device. Refer to [Section 1.7 on page 26](#) for more information on the **RESET** button.

## 25.3 The Reboot Screen

System restart allows you to reboot the Device remotely without turning the power off. You may need to do this if the Device hangs, for example.

Click **Maintenance > Reboot**. Click the **Reboot** button to have the Device reboot. This does not affect the Device's configuration.





## Diagnostic

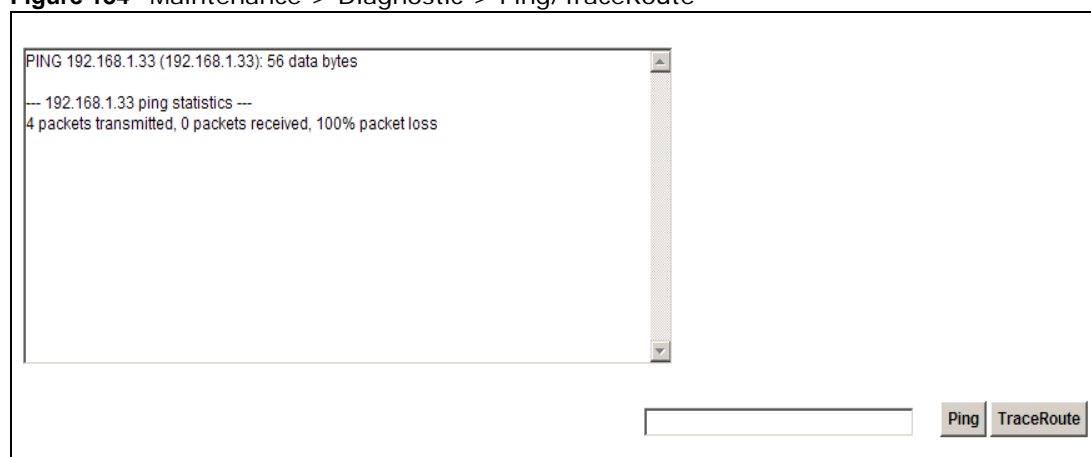
### 26.1 Overview

You can use different diagnostic methods to test a connection and see the detailed information. These read-only screens display information to help you identify problems with the Device.

### 26.2 The Ping/TraceRoute Screen

Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections. Click **Maintenance > Diagnostic** to open the **Ping/TraceRoute** screen shown next.

**Figure 134** Maintenance > Diagnostic > Ping/TraceRoute



The following table describes the fields in this screen.

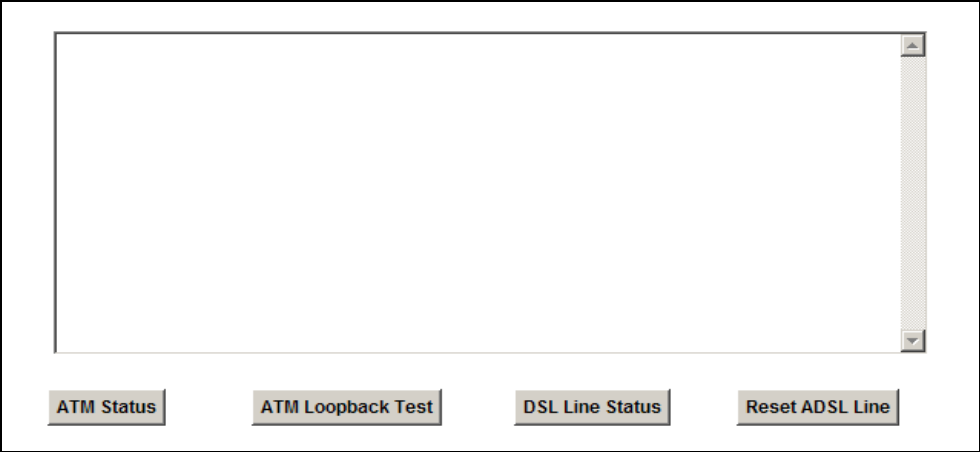
**Table 87** Maintenance > Diagnostic > Ping/TraceRoute

LABEL	DESCRIPTION
Ping	Type the IP address of a computer that you want to ping in order to test a connection. Click <b>Ping</b> and the ping statistics will show in the diagnostic .
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

## 26.3 The DSL Line Screen

Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

**Figure 135** Maintenance > Diagnostic > DSL Line



The following table describes the fields in this screen.

**Table 88** Maintenance > Diagnostic > DSL Line

ITEM	DESCRIPTION
ATM Status	<p>This is available only when your WAN mode is <b>ADSL</b>.</p> <p>Click this button to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed.</p> <p>The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets.</p> <p>These counters are set back to zero whenever the device starts up.</p> <ul style="list-style-type: none"><li>• <b>inPkts</b> is the number of good ATM cells that have been received.</li><li>• <b>inDiscards</b> is the number of received ATM cells that were rejected.</li><li>• <b>outPkts</b> is the number of ATM cells that have been sent.</li><li>• <b>outDiscards</b> is the number of ATM cells sent that were rejected.</li></ul>
ATM Loopback Test	<p>This is available only when your WAN mode is <b>ADSL</b>.</p> <p>Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.</p>

**Table 88** Maintenance > Diagnostic > DSL Line (continued)

ITEM	DESCRIPTION
DSL Line Status	<p>Click this button to view statistics about the DSL connections.</p> <ol style="list-style-type: none"> <li>1. <b>noise margin downstream</b> is the signal to noise ratio for the downstream part of the connection (coming into the Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is.</li> <li>2. <b>output power upstream</b> is the amount of power (in decibels) that the Device is using to transmit to the ISP.</li> <li>3. <b>attenuation downstream</b> is the reduction in amplitude (in decibels) of the DSL signal coming into the Device from the ISP.</li> </ol> <p>Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT.</p> <p>The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.</p>
Reset DSL Line	<p>Click this button to reinitialize the DSL line. The large text box above then displays the progress and results of this operation, for example:</p> <p>"Start to reset ADSL</p> <p>Loading ADSL modem F/W...</p> <p>Reset ADSL Line Successfully!"</p>



# Troubleshooting

## 27.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [Device Access and Login](#)
- [Internet Access](#)
- [Wireless Internet Access](#)
- [Phone Calls and VoIP](#)
- [USB Device Connection](#)
- [UPnP](#)

## 27.2 Power, Hardware Connections, and LEDs

---

[The Device does not turn on. None of the LEDs turn on.](#)

---

- 1 Make sure the Device is turned on.
- 2 Make sure you are using the power adaptor or cord included with the Device.
- 3 Make sure the power adaptor or cord is connected to the Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the Device off and on.
- 5 If the problem continues, contact the vendor.

---

[One of the LEDs does not behave as expected.](#)

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.6 on page 24](#).
- 2 Check the hardware connections. See the Quick Start Guide.

- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the Device off and on.
- 5 If the problem continues, contact the vendor.

## 27.3 Device Access and Login

---

I forgot the IP address for the Device.

---

- 1 The default IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Device (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.7 on page 26](#).

---

I forgot the password.

---

- 1 The default admin password is **1234** and the default user password is **1234**.
- 2 If you can't remember the password, you have to reset the device to its factory defaults. See [Section 1.7 on page 26](#).

---

I cannot see or access the **Login** screen in the web configurator.

---

- 1 Make sure you are using the correct IP address.
  - The default IP address is 192.168.1.1.
  - If you changed the IP address ([Section on page 161](#)), use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Device](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See [Appendix C on page 329](#).

- 4 Reset the device to its factory defaults, and try to access the Device with the default IP address. See [Section 1.7 on page 26](#).
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

### Advanced Suggestions

- Try to access the Device using another service, such as Telnet. If you can access the Device, check the remote management settings and firewall rules to find out why the Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

---

I can see the **Login** screen, but I cannot log in to the Device.

---

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the Device. Log out of the Device in the other session, or ask the person who is logged in to log out.
- 3 Turn the Device off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 27.2 on page 273](#).

---

I cannot Telnet to the Device.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

---

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

## 27.4 Internet Access

---

### I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.6 on page 24](#).
- 2 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 4 If you are trying to access the Internet wirelessly, make sure you have enabled the wireless LAN by the **WPS/WLAN** button or the **Network Setting > Wireless > General** screen.
- 5 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 6 If the problem continues, contact your ISP.

---

### I cannot access the Internet through a DSL connection.

---

- 1 Check if you set the WAN Mode type to **ADSL/VDSL** in the **Broadband** screen to have the Device use the DSL port for Internet access.
- 2 Make sure you configured a proper DSL WAN connection with the Internet account information provided by your ISP.
- 3 If you set up a WAN connection using bridging service (all LAN ports and WLAN BSSs are bridged to one WAN connection), make sure you turn off the DHCP feature in the **Home Networking** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

---

### I cannot access the Internet through an Ethernet WAN connection.

---

- 1 Check if you set the WAN Mode type to **EtherWAN** in the **Broadband** screen to have the Device use the Ethernet WAN port for Internet access.
- 2 Make sure you connect the Ethernet WAN port to a DSL modem or router in your network.
- 3 Make sure you configured a proper Ethernet WAN connection with the Internet account information provided by your ISP.



- 4 If you set up a WAN connection using bridging service (all LAN ports and WLAN BSSs are bridged to one WAN connection), make sure you turn off the DHCP feature in the **Home Networking** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

---

I cannot connect to the Internet using a second DSL connection.

---

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

---

I cannot create multiple connections of the same type.

---

Your WAN interface must enable VLAN and fill each WAN connection with different VLAN IDs.

---

I cannot access the Internet anymore. I had access to the Internet (with the Device), but my Internet connection is not available anymore.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.6 on page 24](#).
- 2 Turn the Device off and on.
- 3 If the problem continues, contact your ISP.

---

The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.6 on page 24](#). If the Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Turn the Device off and on.
- 3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

## 27.5 Wireless Internet Access

---

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

---

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

---

What wireless security modes does my Device support?

---

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your ZyXEL device are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

## 27.6 Phone Calls and VoIP

---

The telephone port won't work or the telephone lacks a dial tone.

---

- 1 Check the telephone connections and telephone wire.

---

I can access the Internet, but cannot make VoIP calls.

---

- 1 The **PHONE** light should come on. Make sure that your telephone is connected to the **PHONE** port.
- 2 You can also check the VoIP status in the **System Info** screen.
- 3 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

## 27.7 USB Device Connection

---

The Device fails to detect my USB device.

---

- 1 Disconnect the USB device.
- 2 Reboot the Device.
- 3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
- 4 Re-connect your USB device to the Device.

## 27.8 UPnP

---

When using UPnP and the Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

---

- 1 Disconnect the Ethernet cable from the Device's LAN port or from your computer.

- 
- 2 Re-connect the Ethernet cable.

---

The **Local Area Connection** icon for UPnP disappears in the screen.

---

Restart your computer.

---

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

---

- 1 Wait more than three minutes.
- 2 Restart the applications.

## Product Specifications

The following tables summarize the Device's hardware and firmware features.

### Hardware Specifications

**Table 89** Hardware Specifications

Dimensions	224(W) x 168.5(D) x 77.5(H) mm
Power Specification	12V at 2.0A DC
Built-in Switch	Four auto-negotiating, MDI/MDI-X Gigabit Ethernet ports
DSL Port	P-2812HNU(L)-F1: One RJ11(6p2c) over POTS (Annex A), Yellow P-2812HNU(L)-F3: One RJ45(8p6c) over ISDN (Annex B)
WAN Port	One RJ-45(8p8c), auto MDI/MDI-X 10/100/1000Base-Tx , Blue
PHONE Ports	Two FXS POTS ports, RJ-11(4p2c)
FXO port ("L" models only)	One FXO (Foreign Exchange Office) lifeline port
RESET Button	To restore factory defaults, hold for more than 5 seconds. To restart/reboot the system, hold for more than 2 seconds.
WLAN/WPS Button	Press and hold for 5 seconds: Turn WPS on or off Press for 1 second: Turn WLAN on or off
USB Port	Two USB v2.0 ports for file sharing, printer server, and 3G WAN backup
Antenna	Two 2 dBi internal antennas
Operation Temperature	0° C ~ 40° C
Storage Temperature	-25° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH
Distance between the centers of the holes (for wall-mounting) on the device's back	132.3 mm
Screw size for wall-mounting	M4 tap

## Firmware Specifications

**Table 90** Firmware Specifications

Default IP Address	http://192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default User Name	admin
Default Password	1234
DHCP Server IP Pool	Starting Address: http://192.168.1.33 Size: 32
Static DHCP Addresses	128 Max
Static Routes	16
Device Management	Use the web configurator to easily configure the rich range of features on the Device.
Wireless Functionality (wireless devices only)	Allow IEEE 802.11n, IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an HTTP/FTP/SCP/SFTP tool to put it on the Device.  Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the Device's configuration. You can put it back on the Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
MAC Address Filtering	Your device can check the MAC addresses of clients against a list of allowed MAC addresses.

**Table 90** Firmware Specifications (continued)

QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the Device.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 7 Permanent Virtual Circuits (PVCs) by default.
VDSL Standards	<p><u>COMPLIANCE</u></p> <ul style="list-style-type: none"> <li>• G.993.2, including Amendments 1-4 and Corrigendum 1-2</li> <li>• WT114 (revision 14 released 2009-01-14): loop reach</li> <li>• WT115 (revision 7 released 2009-02-09) : functionality</li> <li>• TPS-TC function: PTM mode</li> <li>• G993.2 clause 7.2 UPBO (upstream power back-off)</li> <li>• G993.2 clause 12.3 US mask ceiling by using MAXMASKus</li> <li>• VDSL: G.993.1</li> <li>• G.hs: G.994.1</li> <li>• G.997.1</li> <li>• LR-VDSL2</li> </ul>
ADSL Standards	<p><u>COMPLIANCE</u></p> <ul style="list-style-type: none"> <li>• ADSL / 2 / 2+</li> <li>• G.992.5 (ADSL2+) backward compatible with G.992.1 (ADSL G.dmt)</li> <li>• Germany (Annex B/ J) G.992.5 Annex B (ADSL over ISDN)</li> <li>• Sweden (Annex A/ M) G.992.5 Annex A and G.992.5 Annex M</li> <li>• TR-100 A.2-22, A.2-23, B3-14 and B.3.15 (with FSAN noise FB) A.2-20, A.2.21, B3.12 and B.3-13 (with AWGN noise)</li> <li>• ADSL: ANSI T1.413, G.992.1 (G.dmt) Annex A, G.992.2 (G.lite) Annex A, G.994.1 (G.hs)</li> <li>• RE-ADSL (Reach-Extended ADSL)</li> </ul> <p><u>ATM</u></p> <ul style="list-style-type: none"> <li>• F4/F5 OAM</li> <li>• VC-based and LLC-based multiplexing</li> <li>• Multi-protocol over AAL5 (RFC2684)</li> <li>• PPP over ATM AAL5 (RFC2364)</li> <li>• ATM QoS (CBR, VBR-rt/nrt, UBR)</li> <li>• Up to 7 PVC</li> </ul>

**Table 90** Firmware Specifications (continued)

Other Protocol Support	<ul style="list-style-type: none"> <li>• Transparent bridging for unsupported network layer protocols</li> <li>• IP Multicasting IGMP v1, v2, v3</li> <li>• IGMP Proxy/Snooping</li> </ul>
Management	<ul style="list-style-type: none"> <li>• Embedded Web Configurator</li> <li>• CLI (Command Line Interpreter)</li> <li>• Firmware upgrade and configuration file restore through Web/FTP/SCP/SFTP</li> <li>• Remote Management Control: Telnet, FTP, Web, SSH/SCP/SFTP, and ICMP.</li> <li>• Remote Firmware Upgrade</li> <li>• Syslog</li> <li>• TR-069</li> <li>• TR-064</li> </ul>

## Voice Specifications

Note: To take full advantage of the supplementary phone services available through the Device's phone port, you may need to subscribe to the services from your VoIP service provider.

Note: Not all features are supported by all service providers. Consult your service provider for more information.

**Table 91** Voice Features

Voice over IP	SIP standard (RFC3261), as well as phone features. TYPE-II CPEs support 2 FXS ports design which allows users to make 2 VoIP phone calls at the same time.
Multiple SIP Accounts	You can simultaneously use multiple voice (SIP) accounts and assign them to the telephone port (up to two accounts).
Echo Cancellation	Your device supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.
Voice Activity Detection/Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Caller ID	The Device supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display).
Call Return	With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN.
Multiple Voice Channels	Your device can simultaneously handle multiple voice channels (telephone calls). Additionally you can answer an incoming phone call on a VoIP account, even while someone else is using the account for a phone call.
Call waiting	This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call.



**Table 91** Voice Features (continued)

Call forwarding	With this feature, you can set the Device to forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network.
Other Voice Features	<p>SIP version 2 (Session Initiation Protocol RFC 3261)</p> <p>SDP (Session Description Protocol RFC 2327, 3264, 4566 )</p> <p>RTP/RTCP (RFC 3550)</p> <p>Voice codecs (coder/decoders) G.711, G.729ab, G.722, G.726</p> <p>Fax and data modem discrimination</p> <p>DTMF Detection and Generation</p> <p>DTMF: In-band and Out-band traffic (RFC 2833)</p> <p>Quick dialing through predefined phone book, which maps the phone dialing number and destination URL.</p>

## Wireless Features

**Table 92** Wireless Features

Internal Antenna	The Device is equipped with two internal antennas to provide a clear radio signal between the wireless stations and the access points.
Multiple SSID	Multiple SSID allows the Device to operate up to 4 different wireless networks simultaneously, each with independently configurable wireless and security settings.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
WPS	Wi-Fi Protected Setup
Other Wireless Features	<p>IEEE 802.11n Compliance</p> <p>Frequency Range: 802.11b/g/n ISM Band: 2.4 GHz</p> <p>Turn on-off WLAN by <b>WLAN</b> button (press the <b>WLAN</b> button for one second to turn the WLAN on or turn off)</p> <p>IEEE 802.11e</p> <p>Wired Equivalent Privacy (WEP) Data Encryption 64/128 bit</p> <p>WLAN bridge to DSL/Ethernet WAN</p> <p>IEEE 802.1x</p> <p>External RADIUS server</p>

The following list, which is not exhaustive, illustrates the standards supported in the Device.

**Table 93** Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 2236	Internet Group Management Protocol, Version 2
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802)
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11n	Uses the 2.4 gigahertz (GHz) band and 5 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
802.1x	Port Based Network Access Control
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
TR-069	TR-069 DSL Forum Standard for CPE Wan Management
TR-064	DSL Forum LAN-Side DSL CPE Configuration
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)

## Wall-mounting Instructions

Do the following to hang your Device on a wall.

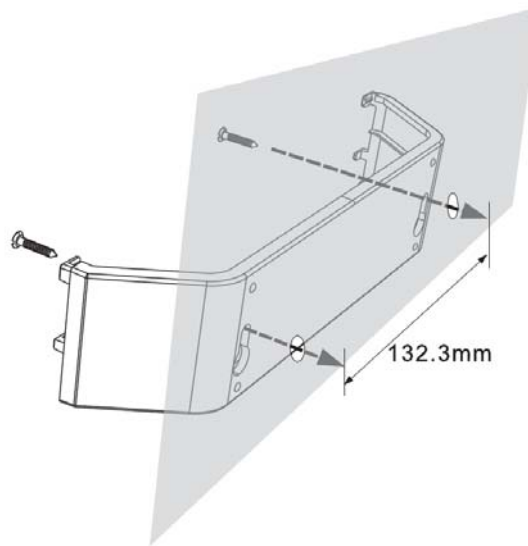
Note: See [Table 89 on page 281](#) for the size of screws to use and how far apart to place them.

- 1 Align the holes on the back of the supplied wall-mounting bracket with the screws. on the wall.
- 2 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.
- 3 Drill two holes on the wall with screws inserted in the wall-mounting bracket. The distance between the screws is 132.3mm.

**Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.**

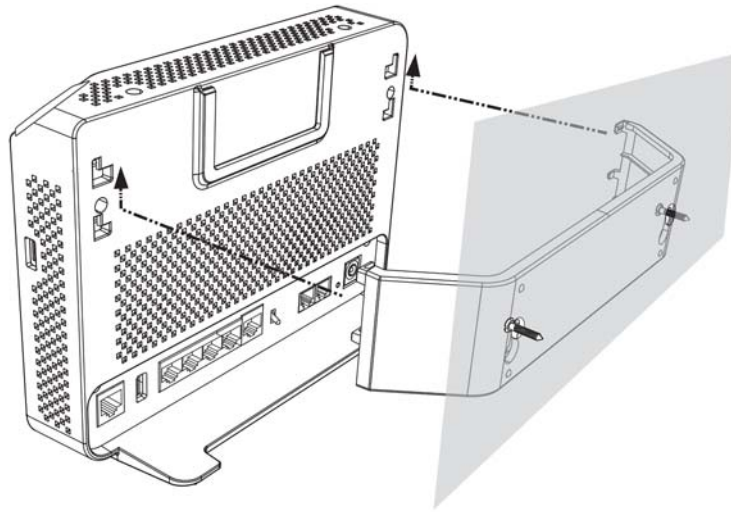
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the Device with the connection cables.

**Figure 136** Wall-mounting -1



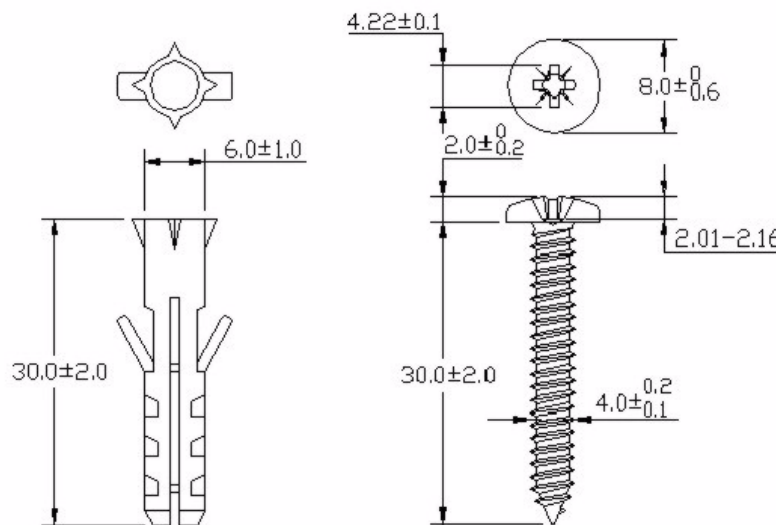
- 5 Mount the Device on the wall-mounting bracket, which is already installed on the wall. Make sure that the Device is firmly attached to the bracket so it does not fall off.

**Figure 137** Wall-mounting -2



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

**Figure 138** Masonry Plug and M4 Tap Screw



# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (such as computers, servers, routers, and printers) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

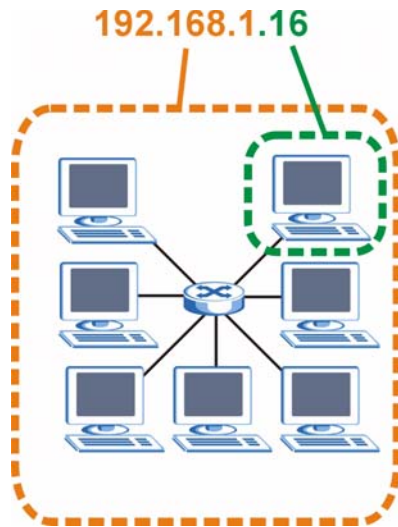
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 139** Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 94** IP Address Network Number and Host ID Example

	<b>1ST OCTET:</b> <b>(192)</b>	<b>2ND OCTET:</b> <b>(168)</b>	<b>3RD OCTET:</b> <b>(1)</b>	<b>4TH OCTET</b> <b>(2)</b>
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	<b>11111111</b>	<b>11111111</b>	<b>11111111</b>	00000000
Network Number	<b>11000000</b>	<b>10101000</b>	<b>00000001</b>	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 95** Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 96** Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 97** Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

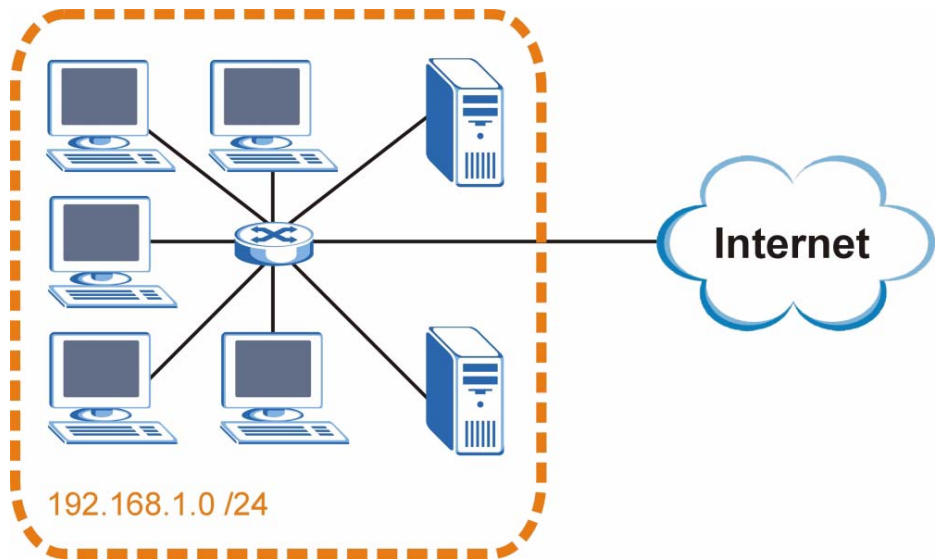
## Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of  $2^8 - 2$  or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 140** Subnetting Example: Before Subnetting



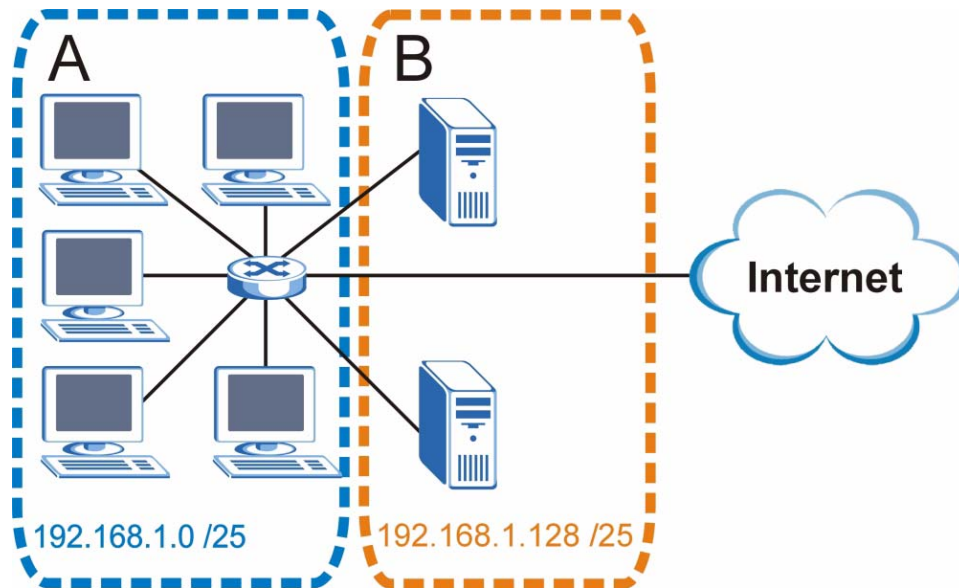
You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.



The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 141** Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of  $2^7 - 2$  or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving  $2^6 - 2$  or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 98** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000

**Table 98** Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 99** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 100** Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 101** Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 102** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 103** 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 104** 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14

**Table 104** 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

## Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Device.

Once you have decided on the network number, pick an IP address for your Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

## Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

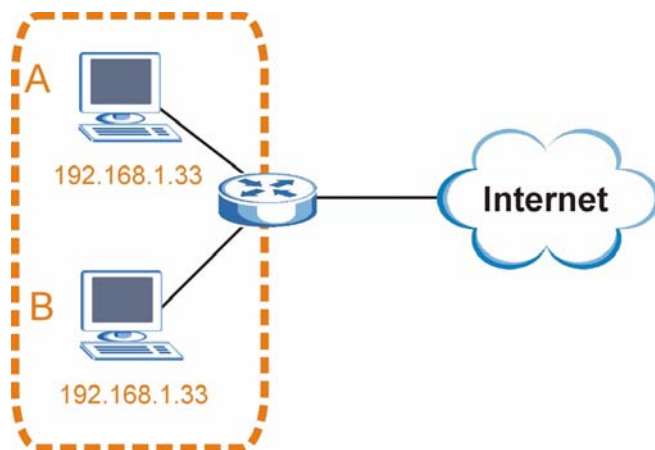
## IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

### Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

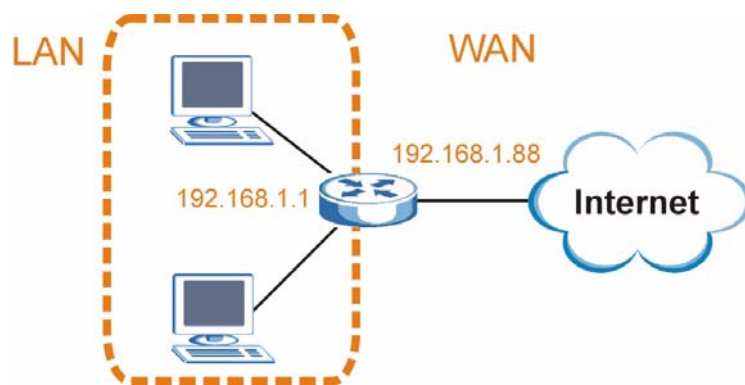
**Figure 142** Conflicting Computer IP Addresses Example



### Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

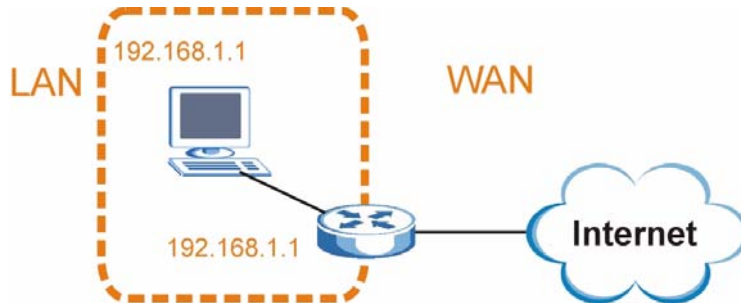
**Figure 143** Conflicting Computer IP Addresses Example



## Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

**Figure 144** Conflicting Computer and Router IP Addresses Example



# Setting Up Your Computer's IP Address

Note: Your specific Device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

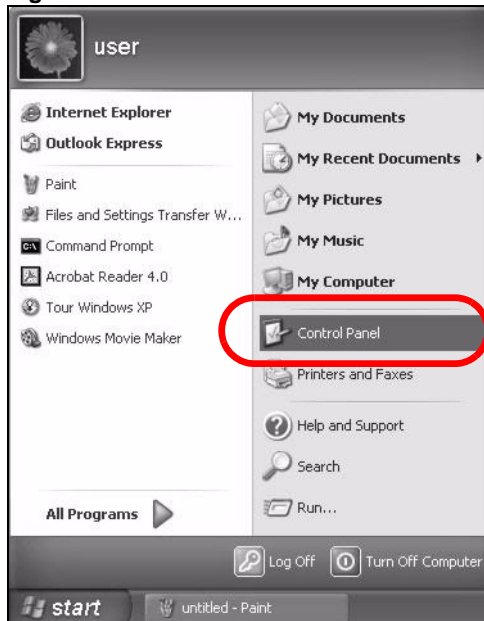
- [Windows XP/NT/2000](#) on [page 299](#)
- [Windows Vista](#) on [page 303](#)
- [Windows 7](#) on [page 307](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 311](#)
- [Mac OS X: 10.5](#) on [page 314](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 318](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 322](#)

## Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

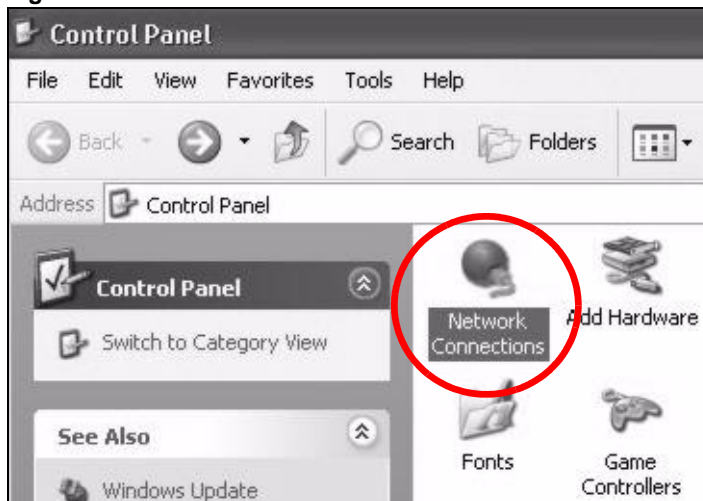
- 1 Click **Start > Control Panel**.

**Figure 145** Windows XP: Start Menu



- 2 In the **Control Panel**, click the **Network Connections** icon.

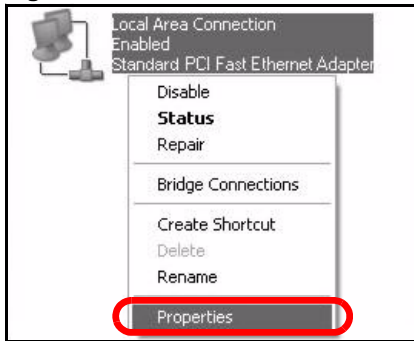
**Figure 146** Windows XP: Control Panel





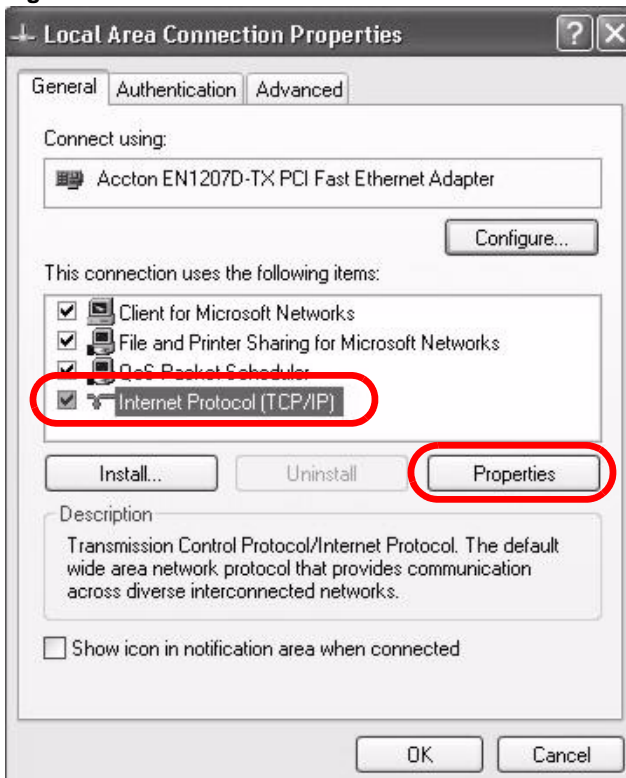
- 3 Right-click **Local Area Connection** and then select **Properties**.

**Figure 147** Windows XP: Control Panel > Network Connections > Properties



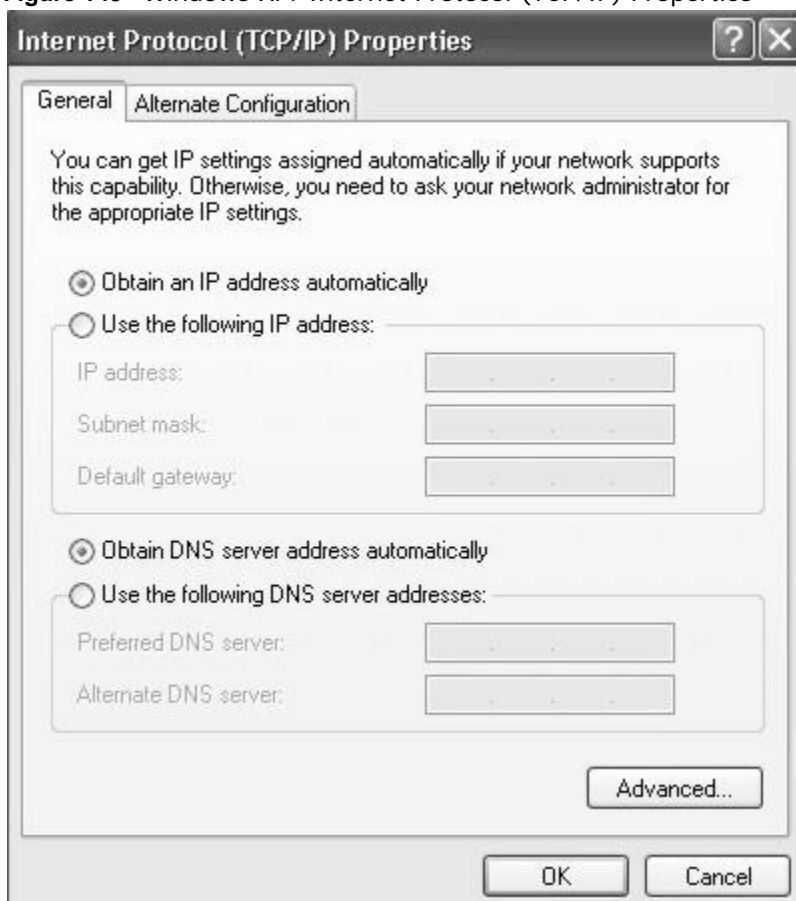
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

**Figure 148** Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens.

**Figure 149** Windows XP: Internet Protocol (TCP/IP) Properties



- 6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

- 7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 8 Click **OK** to close the **Local Area Connection Properties** window.

## Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

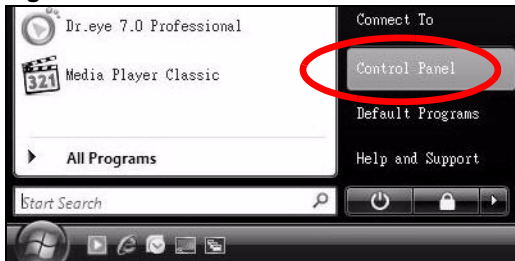
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

## Windows Vista

This section shows screens from Windows Vista Professional.

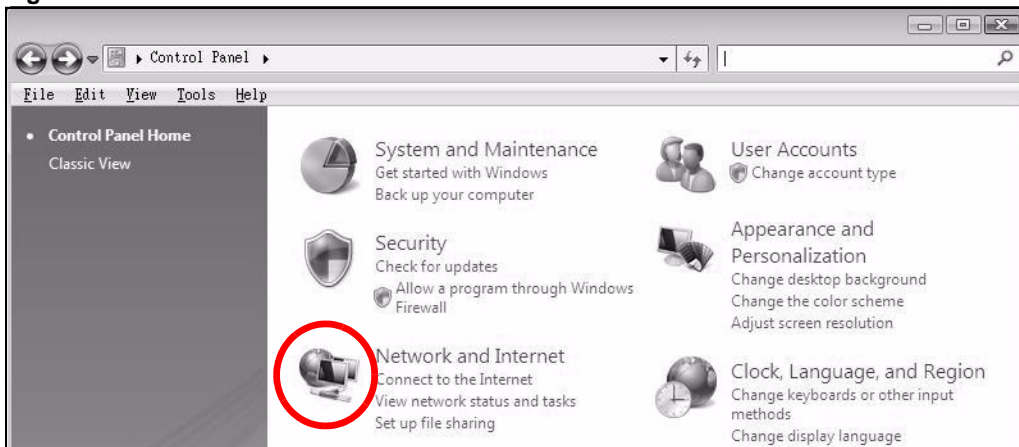
- 1 Click **Start > Control Panel**.

**Figure 150** Windows Vista: Start Menu



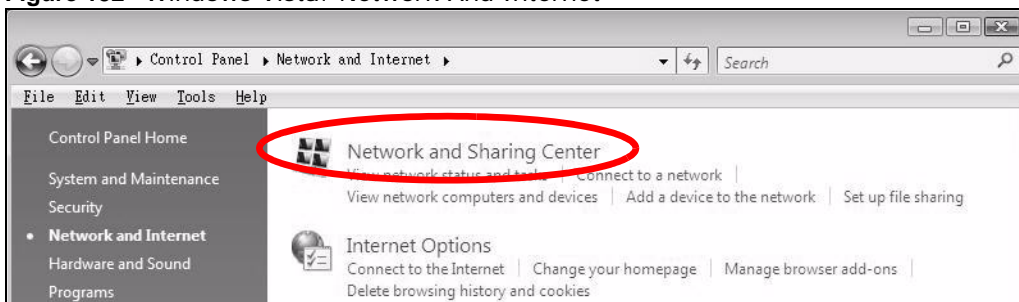
- 2 In the **Control Panel**, click the **Network and Internet** icon.

**Figure 151** Windows Vista: Control Panel



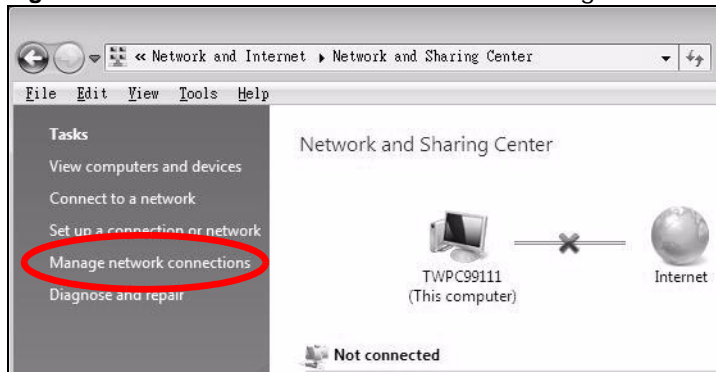
- 3 Click the **Network and Sharing Center** icon.

**Figure 152** Windows Vista: Network And Internet



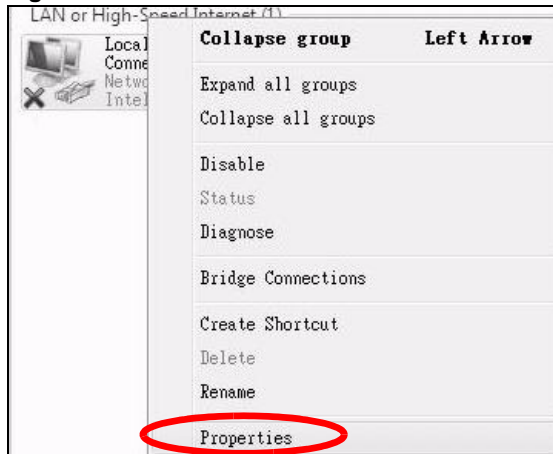
- 4 Click **Manage network connections**.

**Figure 153** Windows Vista: Network and Sharing Center



- 5 Right-click **Local Area Connection** and then select **Properties**.

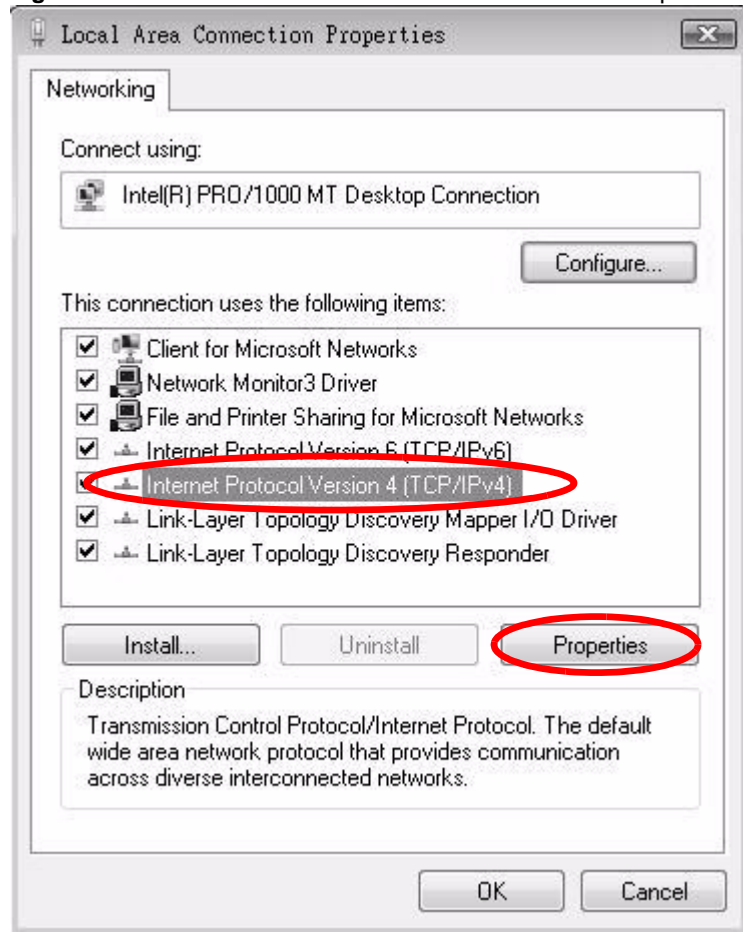
**Figure 154** Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

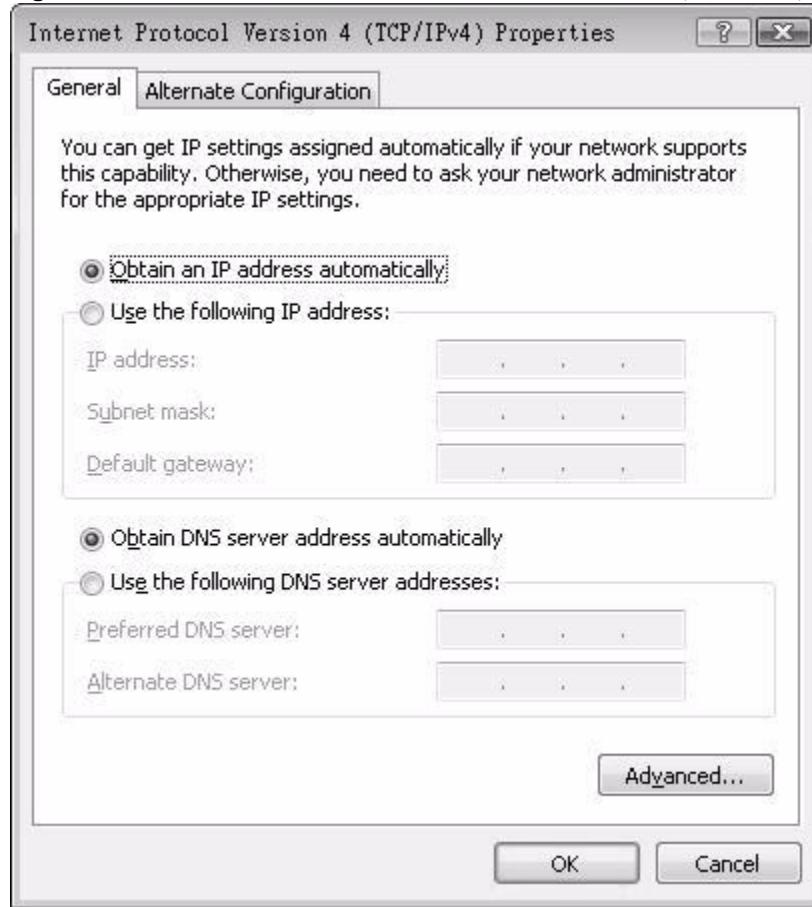
- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

**Figure 155** Windows Vista: Local Area Connection Properties



- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

**Figure 156** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



- 8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced**.

- 9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 10 Click **OK** to close the **Local Area Connection Properties** window.

## Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

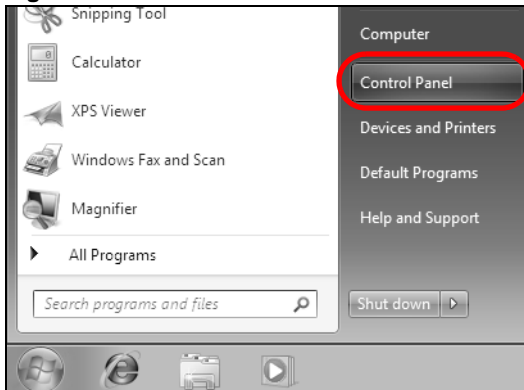
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

## Windows 7

This section shows screens from Windows 7 Enterprise.

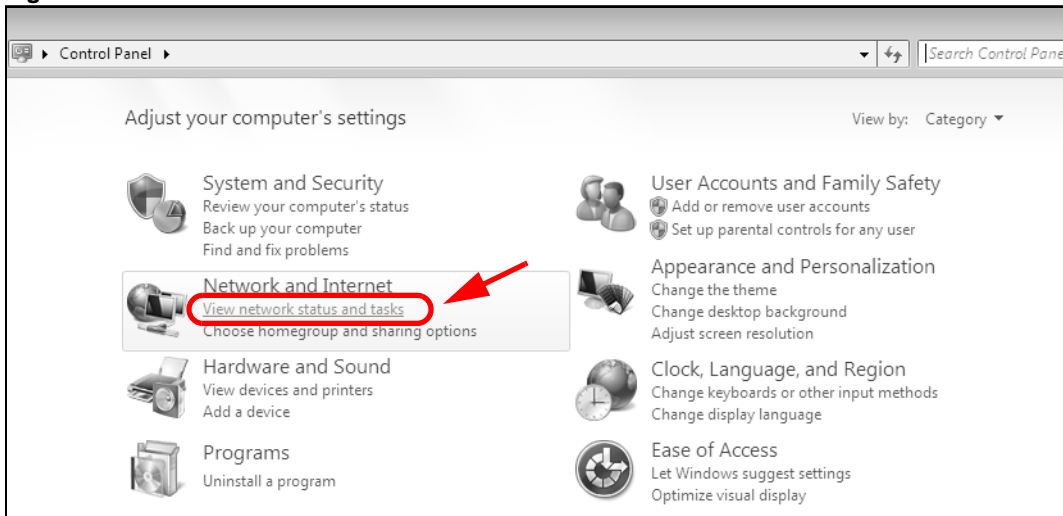
- 1 Click **Start > Control Panel**.

**Figure 157** Windows 7: Start Menu



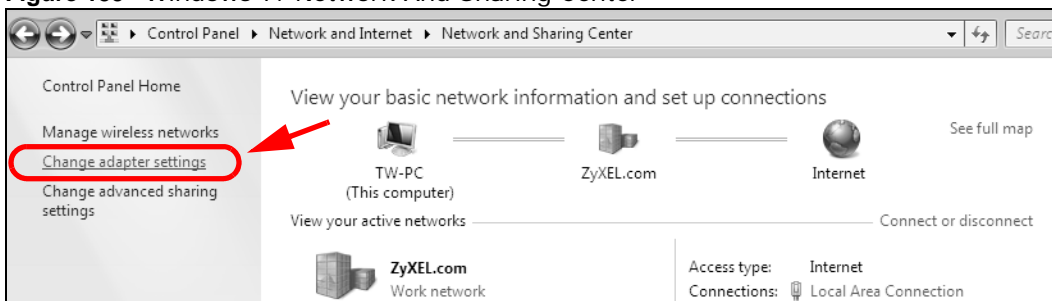
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

**Figure 158** Windows 7: Control Panel



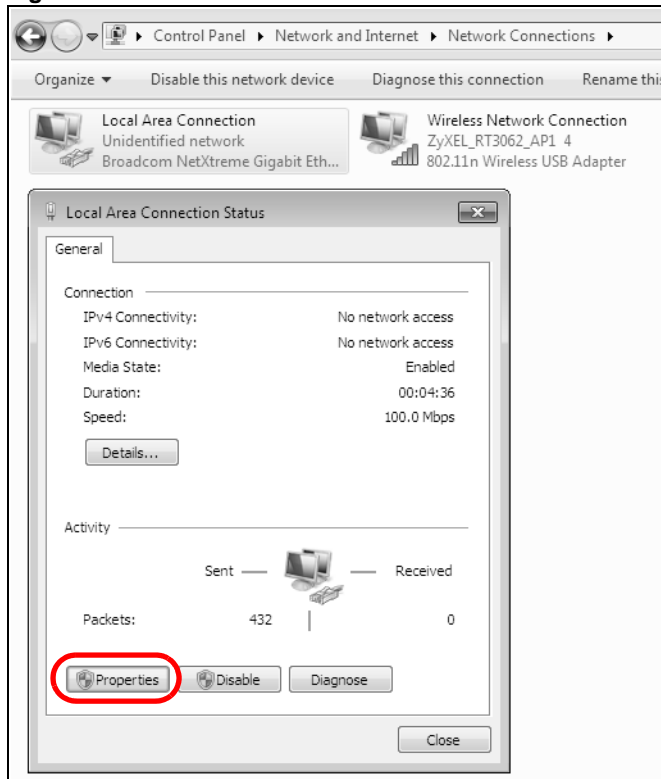
- 3 Click **Change adapter settings**.

**Figure 159** Windows 7: Network And Sharing Center



- 4 Double click **Local Area Connection** and then select **Properties**.

**Figure 160** Windows 7: Local Area Connection Status

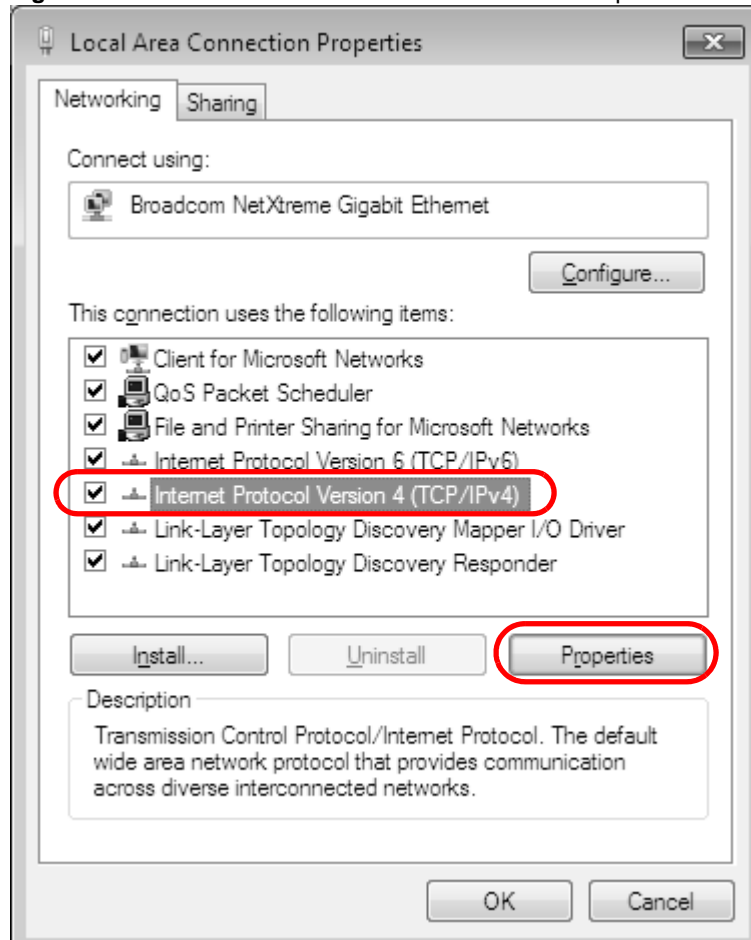


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.



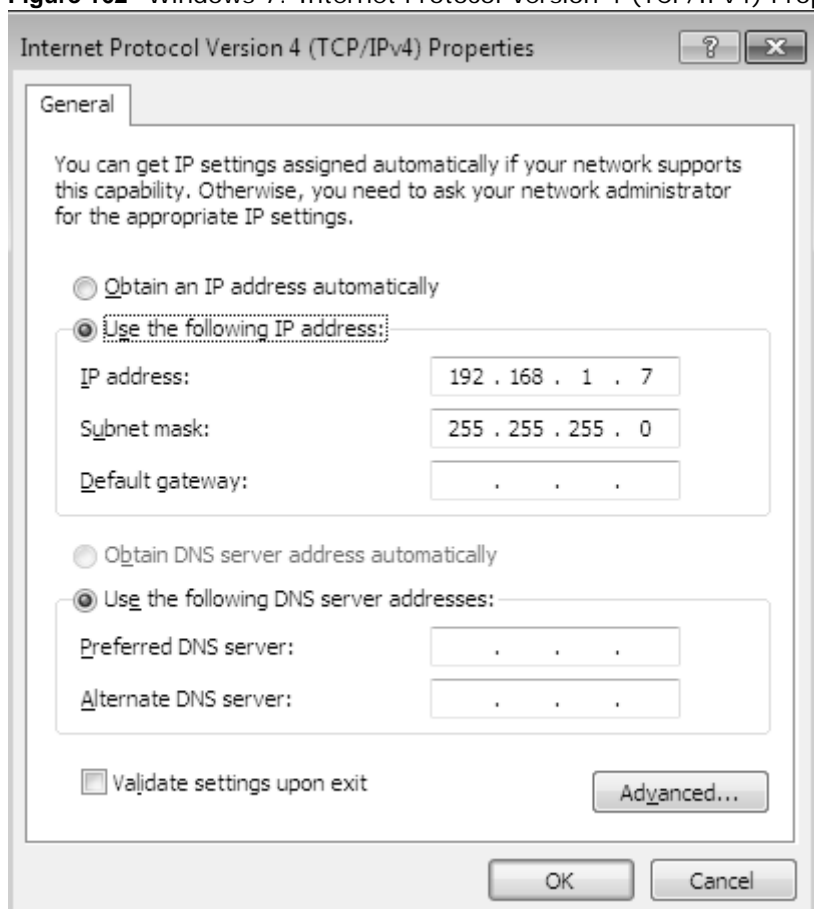
- 5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

**Figure 161** Windows 7: Local Area Connection Properties



- 6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

**Figure 162** Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties



- 7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

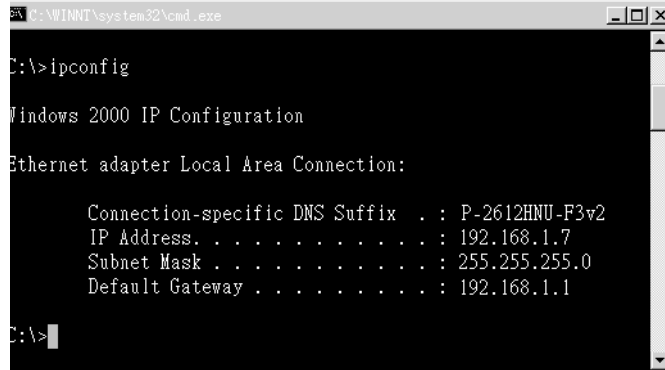
- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **OK** to close the **Local Area Connection Properties** window.

## Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

- 3 The IP settings are displayed as follows.

**Figure 163** Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties



## Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

- 1 Click **Apple > System Preferences**.

**Figure 164** Mac OS X 10.4: Apple Menu



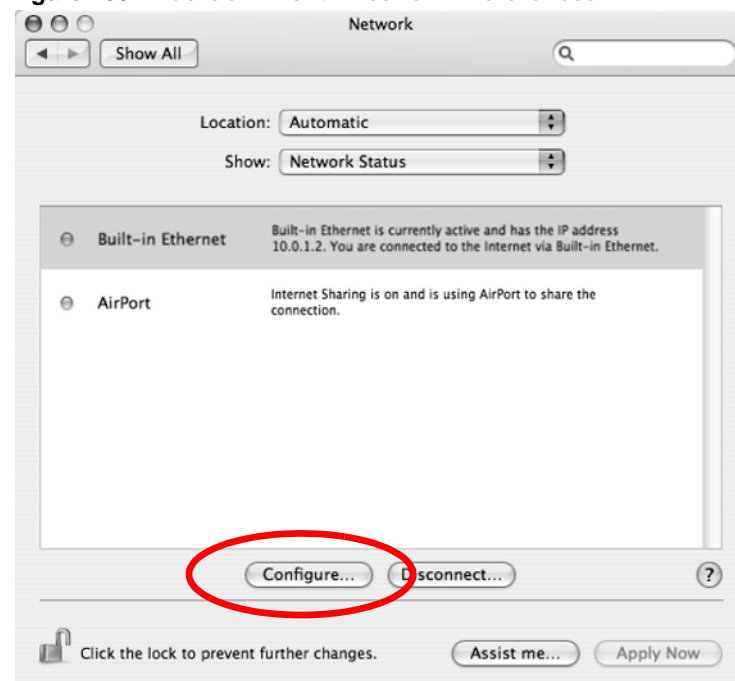
- 2 In the **System Preferences** window, click the **Network** icon.

**Figure 165** Mac OS X 10.4: System Preferences



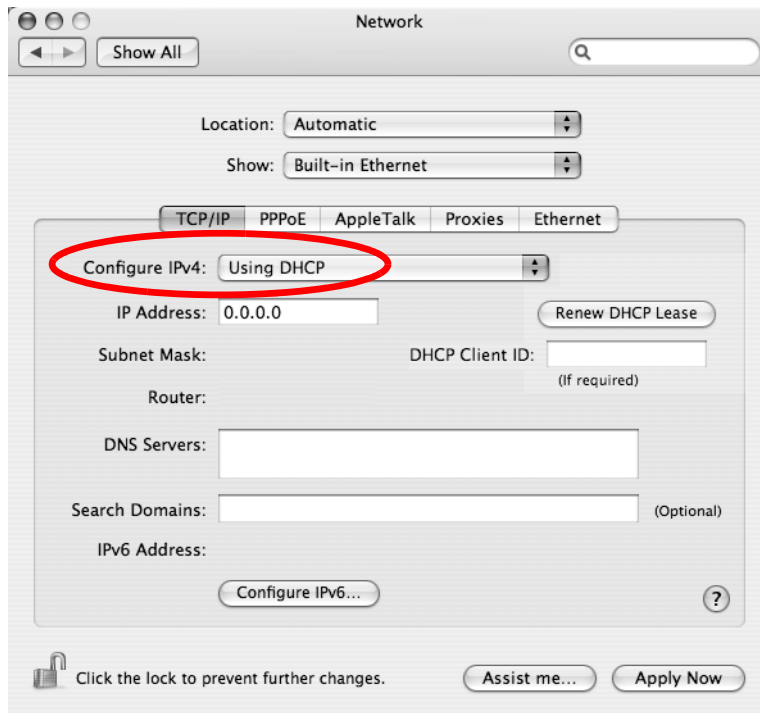
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

**Figure 166** Mac OS X 10.4: Network Preferences



- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

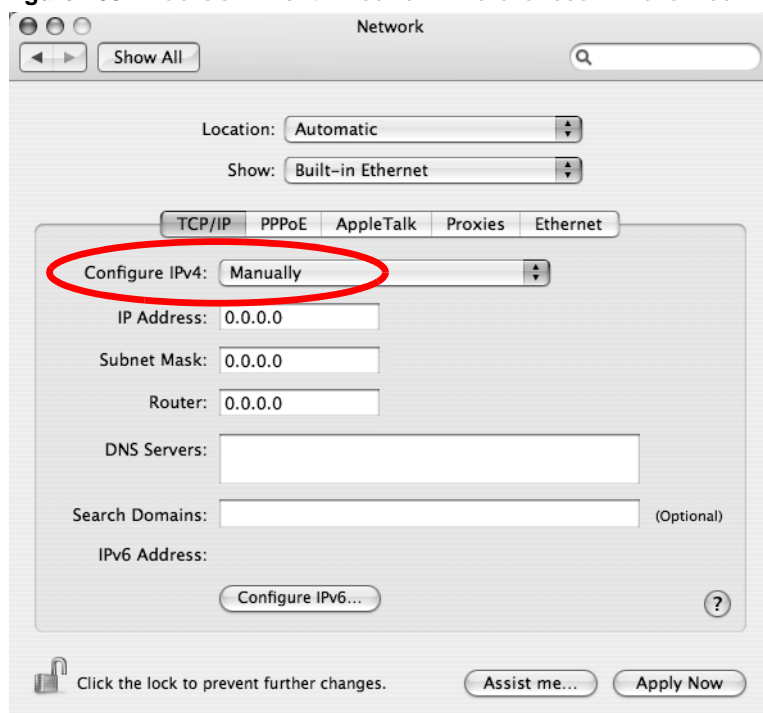
**Figure 167** Mac OS X 10.4: Network Preferences > TCP/IP Tab.



- 5 For statically assigned settings, do the following:
  - From the **Configure IPv4** list, select **Manually**.
  - In the **IP Address** field, type your IP address.
  - In the **Subnet Mask** field, type your subnet mask.

- In the **Router** field, type the IP address of your device.

**Figure 168** Mac OS X 10.4: Network Preferences > Ethernet

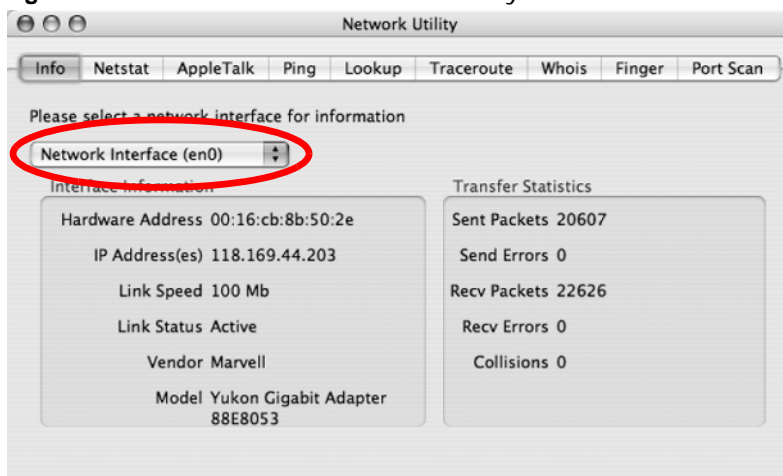


- 6 Click **Apply Now** and close the window.

## Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

**Figure 169** Mac OS X 10.4: Network Utility

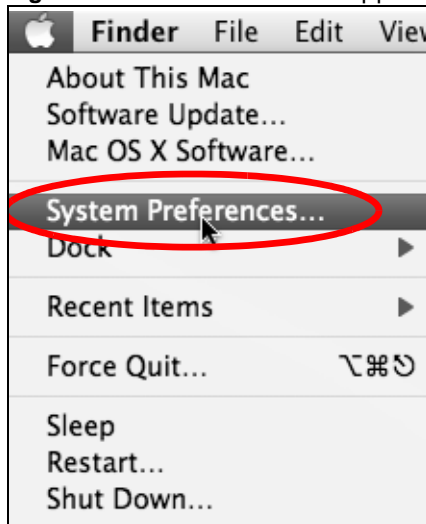


## Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

- 1 Click **Apple** > **System Preferences**.

**Figure 170** Mac OS X 10.5: Apple Menu



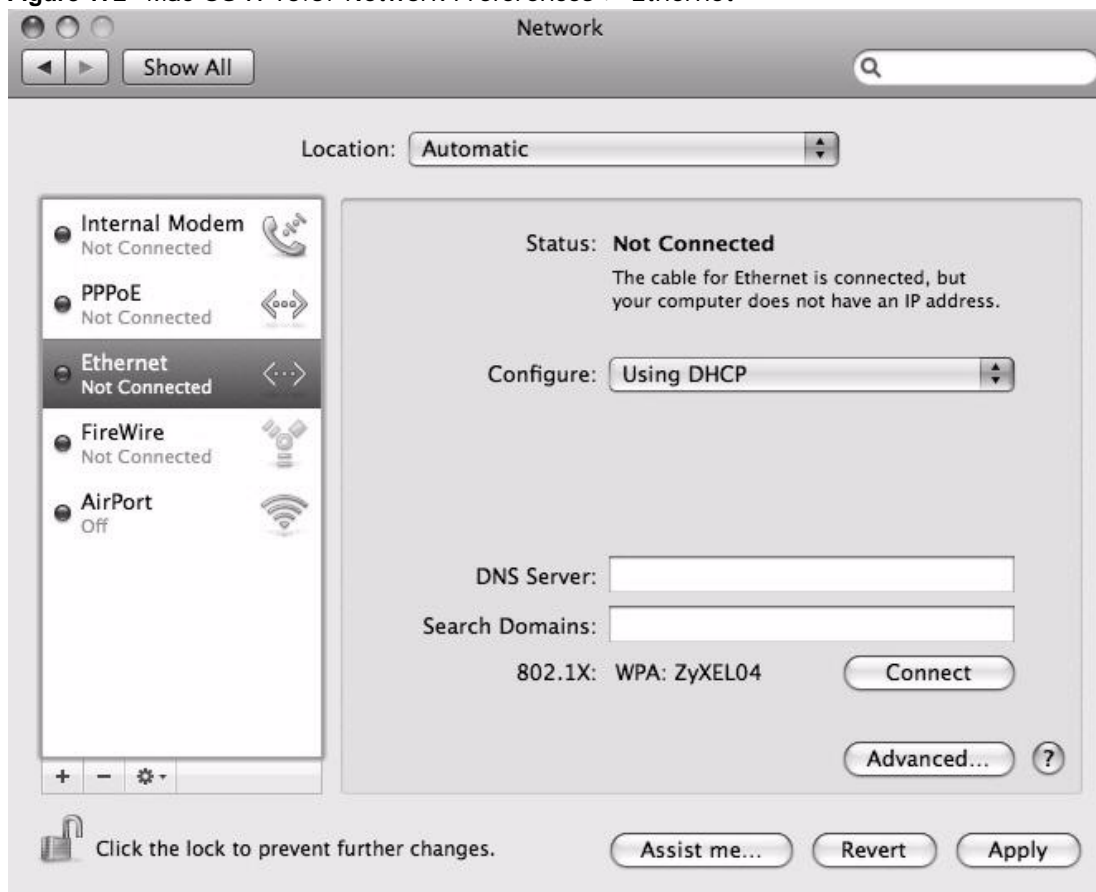
- 2 In **System Preferences**, click the **Network** icon.

**Figure 171** Mac OS X 10.5: Systems Preferences



- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

**Figure 172** Mac OS X 10.5: Network Preferences > Ethernet

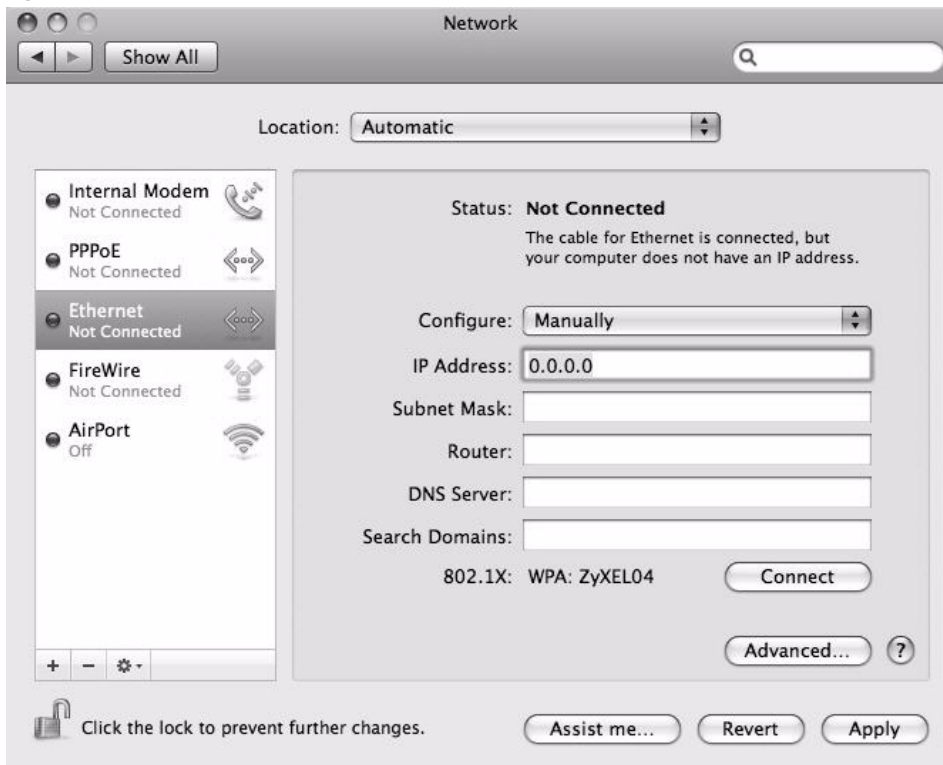


- 4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.
- 5 For statically assigned settings, do the following:
  - From the **Configure** list, select **Manually**.
  - In the **IP Address** field, enter your IP address.
  - In the **Subnet Mask** field, enter your subnet mask.



- In the **Router** field, enter the IP address of your Device.

**Figure 173** Mac OS X 10.5: Network Preferences > Ethernet

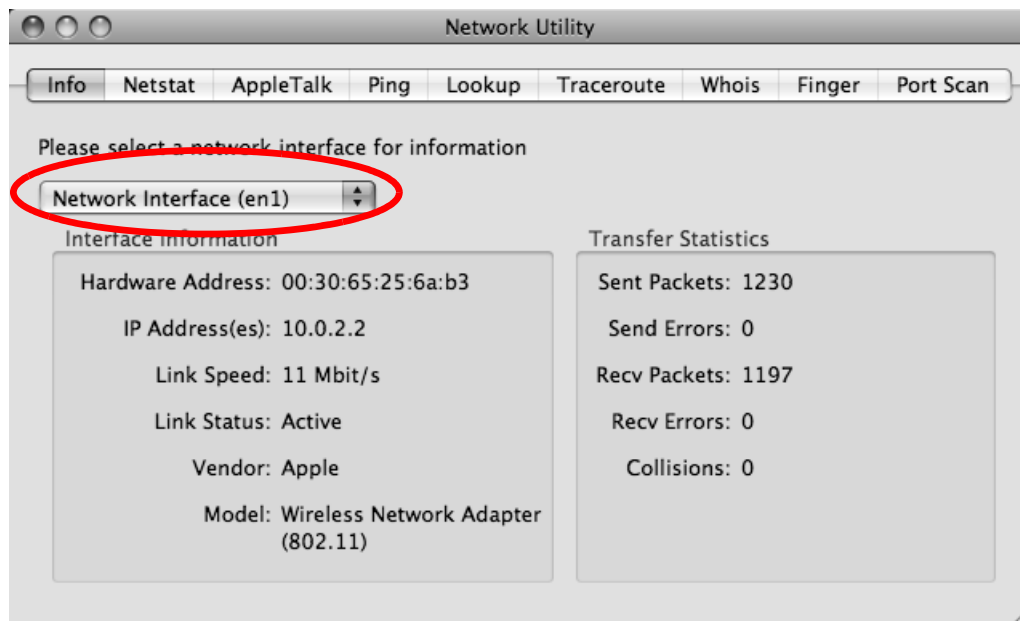


- 6 Click **Apply** and close the window.

## Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

**Figure 174** Mac OS X 10.5: Network Utility



## Linux: Ubuntu 8 (GNOME)

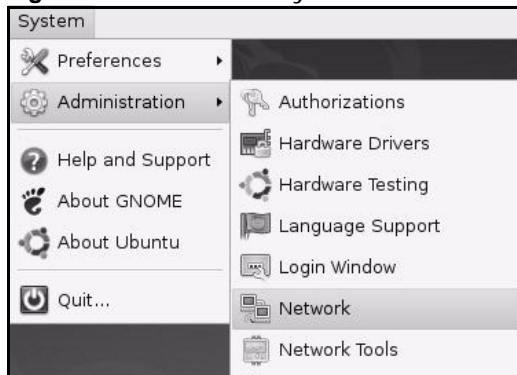
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

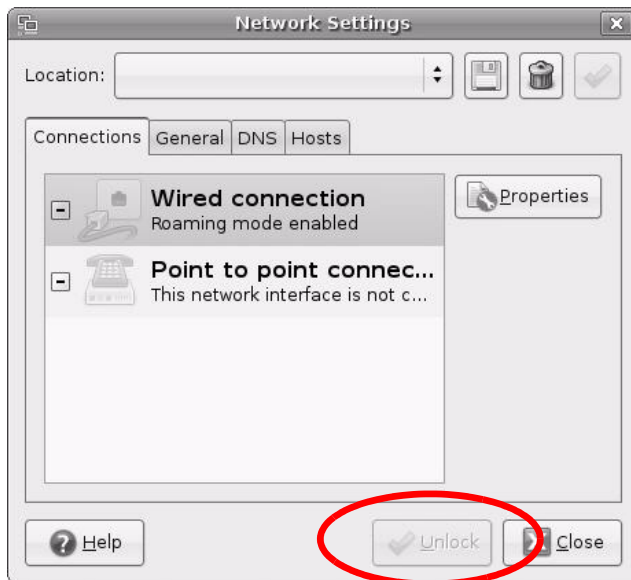
- 1 Click **System > Administration > Network**.

**Figure 175** Ubuntu 8: System > Administration Menu



- 2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

**Figure 176** Ubuntu 8: Network Settings > Connections



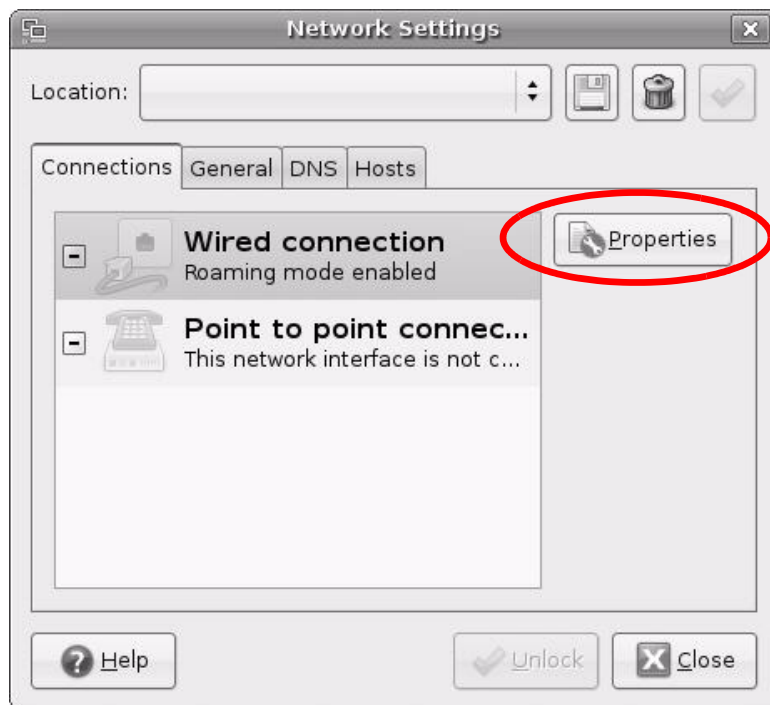
- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

**Figure 177** Ubuntu 8: Administrator Account Authentication



- 4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

**Figure 178** Ubuntu 8: Network Settings > Connections



- 5 The **Properties** dialog box opens.

**Figure 179** Ubuntu 8: Network Settings > Properties



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
  - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

- 7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

**Figure 180** Ubuntu 8: Network Settings > DNS

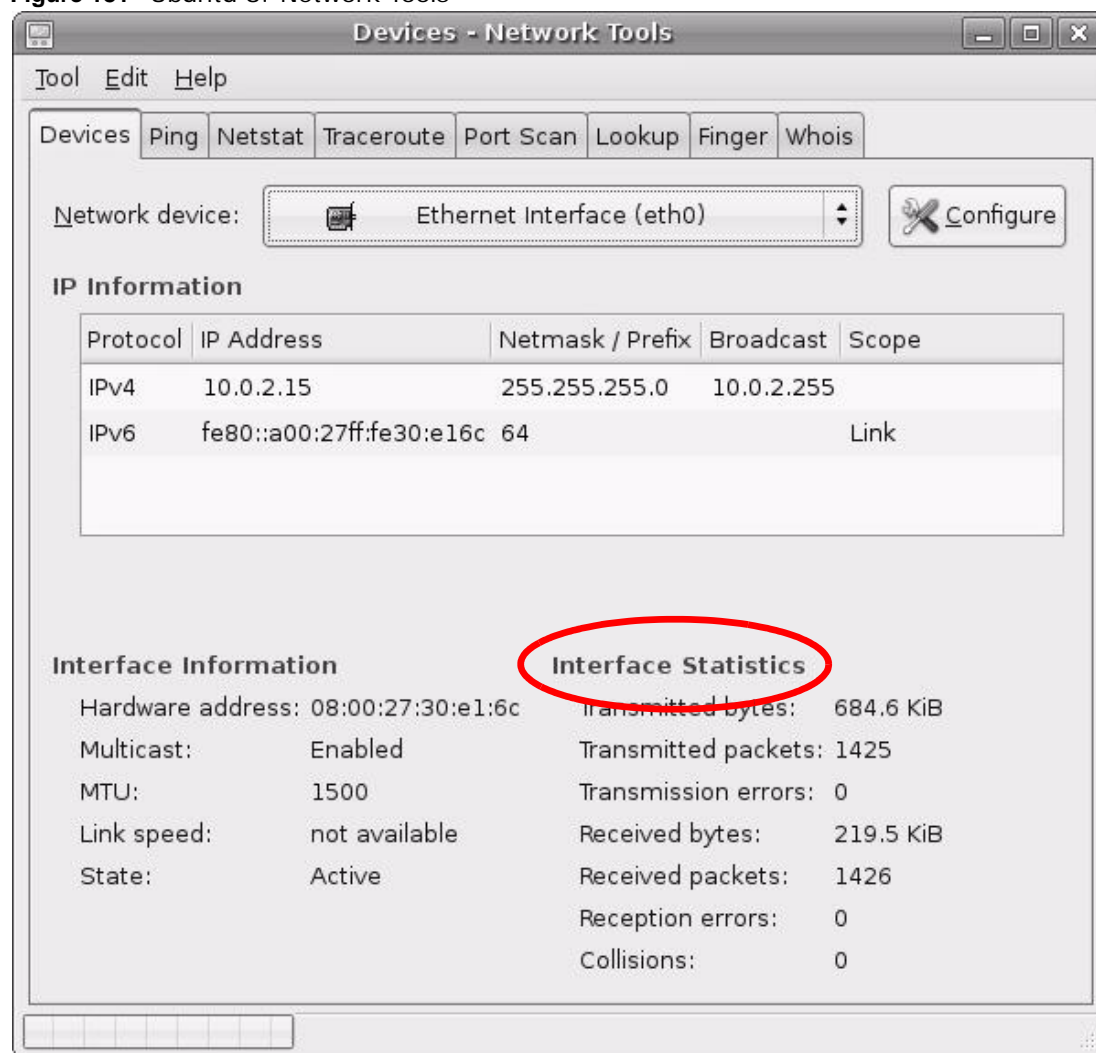


- 8 Click the **Close** button to apply the changes.

## Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

**Figure 181** Ubuntu 8: Network Tools



## Linux: openSUSE 10.3 (KDE)

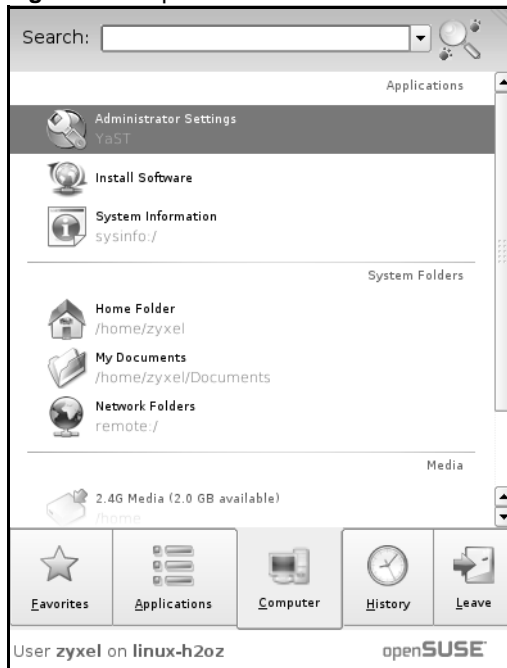
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

**Note:** Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

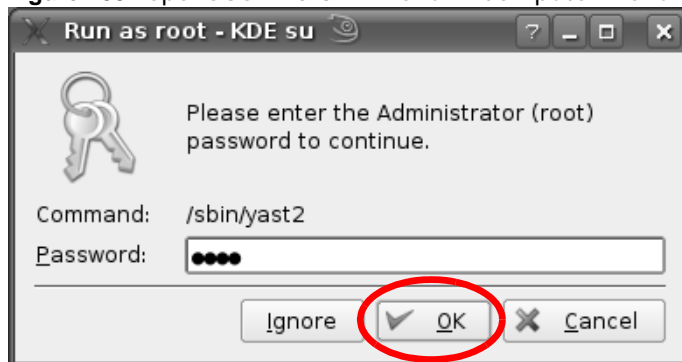
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.

**Figure 182** openSUSE 10.3: K Menu > Computer Menu



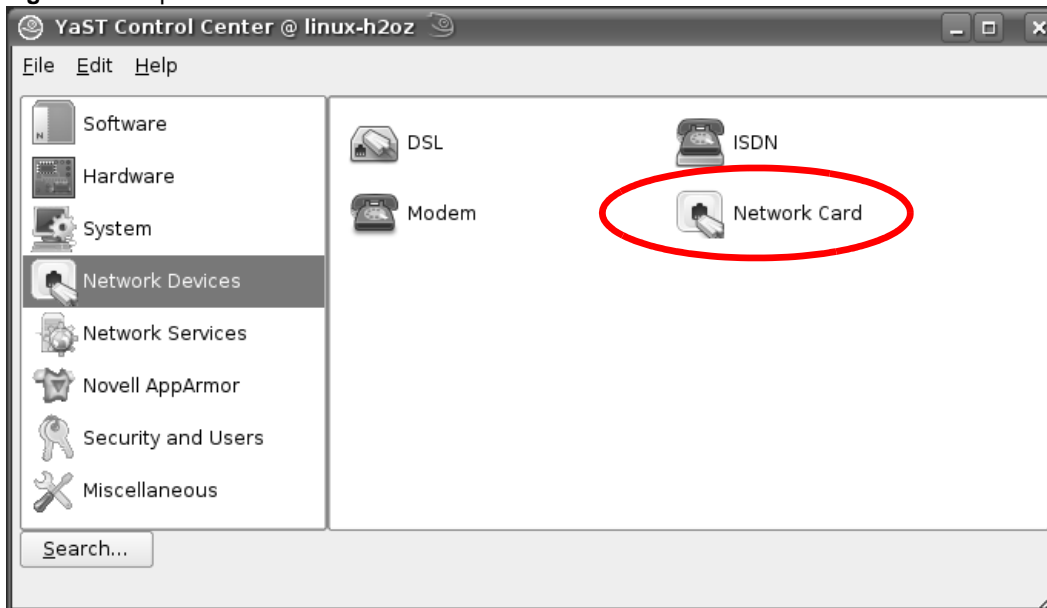
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

**Figure 183** openSUSE 10.3: K Menu > Computer Menu



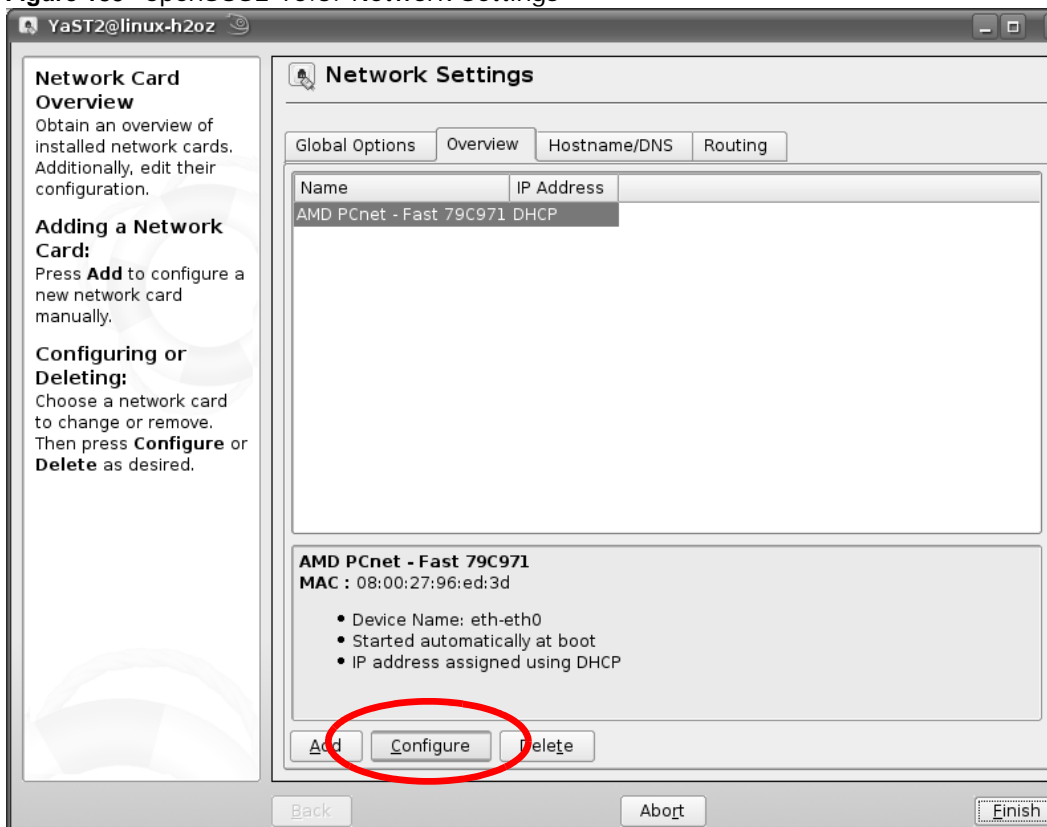
- When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

**Figure 184** openSUSE 10.3: YaST Control Center



- When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

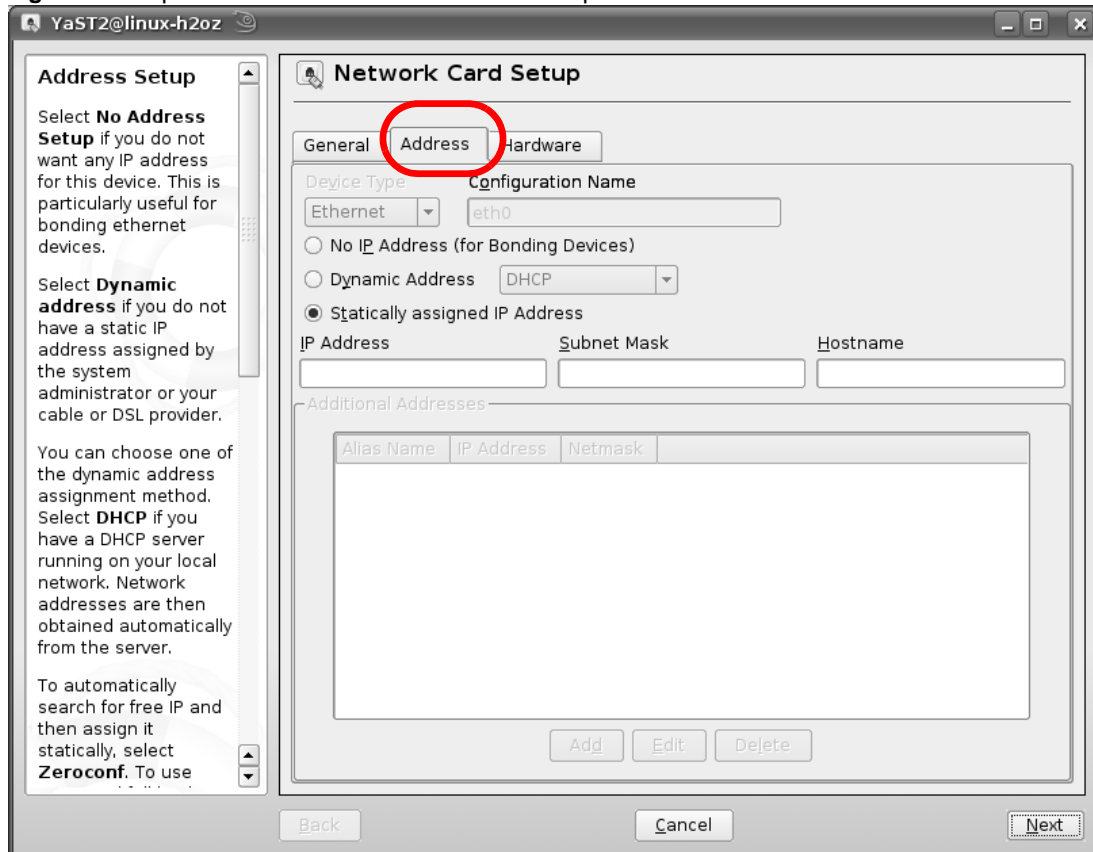
**Figure 185** openSUSE 10.3: Network Settings





- 5 When the **Network Card Setup** window opens, click the **Address** tab

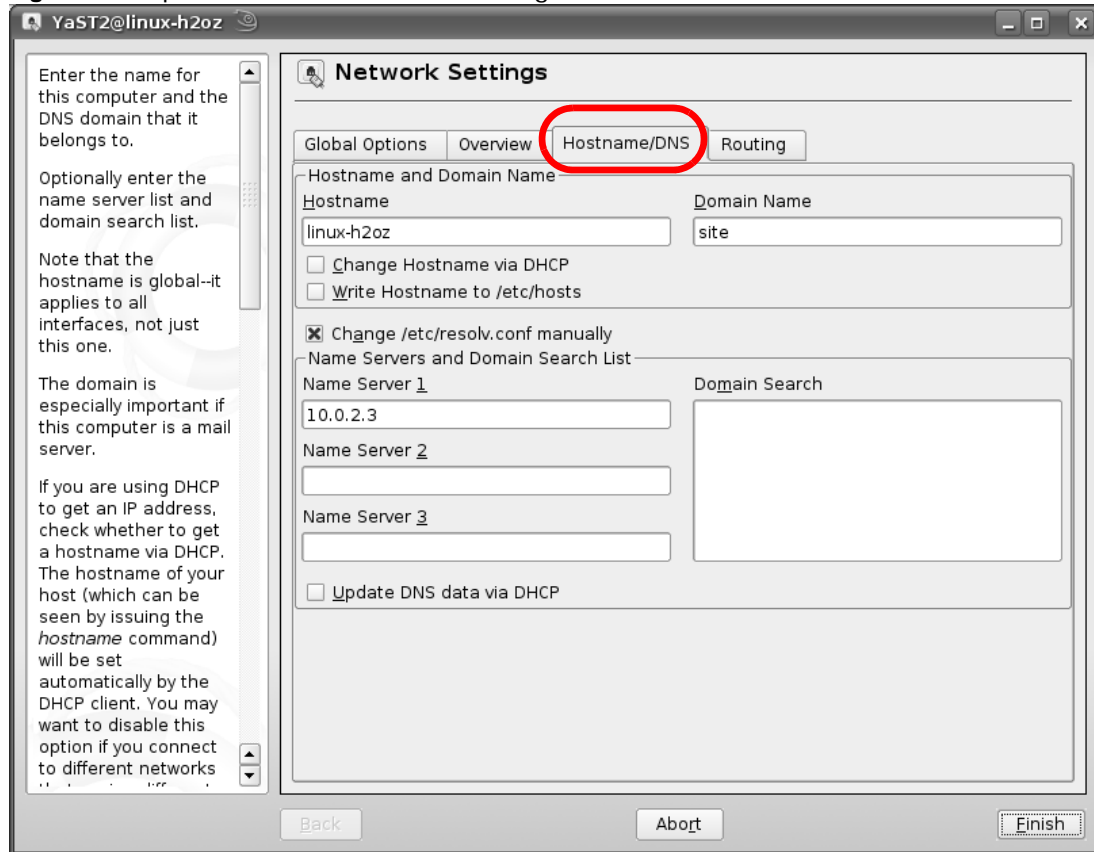
**Figure 186** openSUSE 10.3: Network Card Setup



- 6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.  
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.

- 8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

**Figure 187** openSUSE 10.3: Network Settings

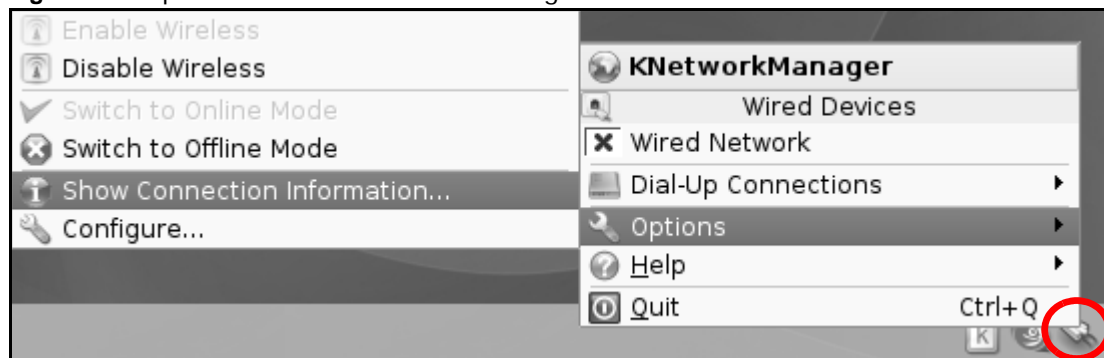


- 9 Click **Finish** to save your settings and close the window.

## Verifying Settings

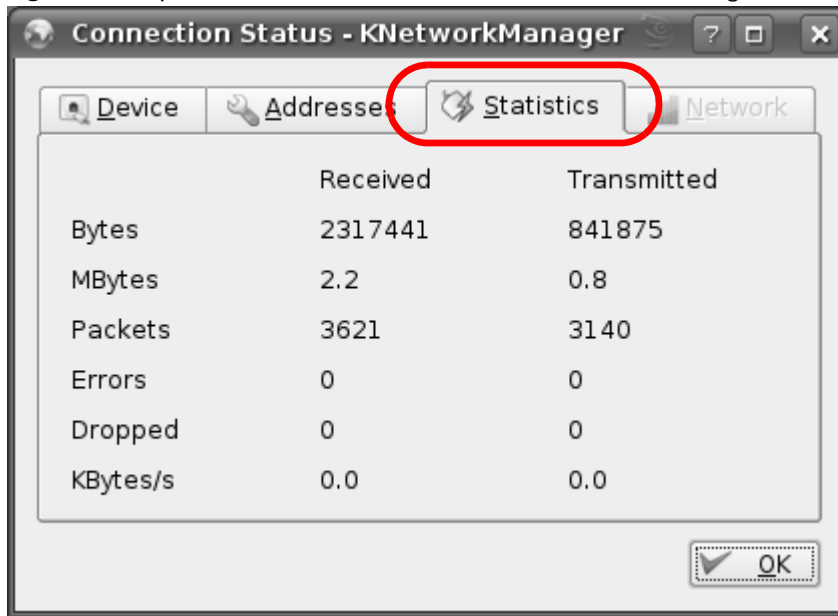
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 188** openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics** tab to see if your connection is working properly.

**Figure 189** openSUSE: Connection Status - KNetwork Manager





# Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

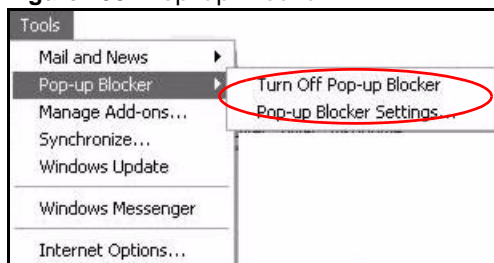
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

## Disable Pop-up Blockers

- 1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 190** Pop-up Blocker

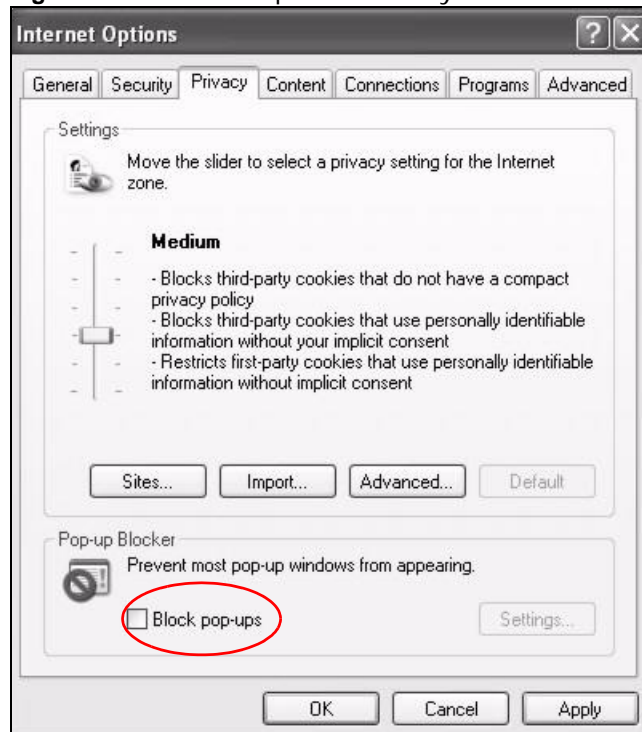


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 191** Internet Options: Privacy



- 3 Click **Apply** to save this setting.

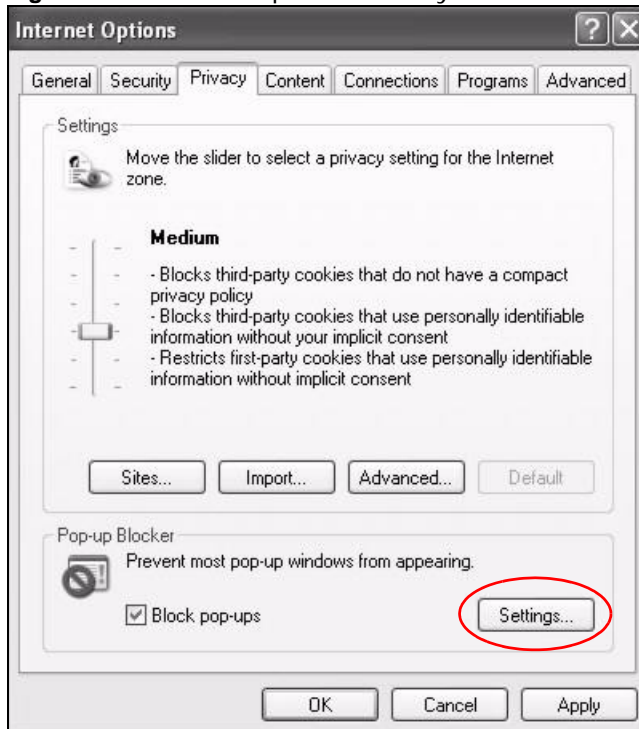
## Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

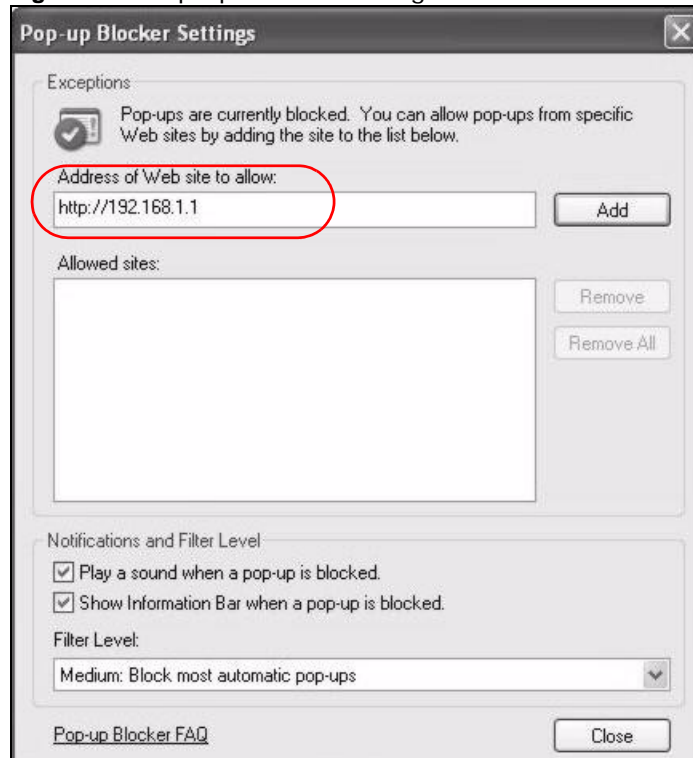
**Figure 192** Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

- Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 193** Pop-up Blocker Settings



- Click **Close** to return to the **Privacy** screen.
- Click **Apply** to save this setting.

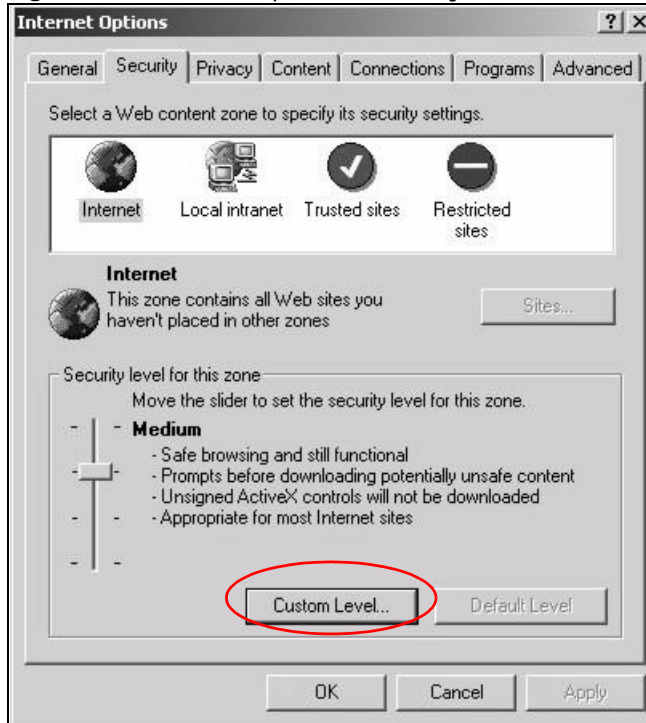
## JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.



- 1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

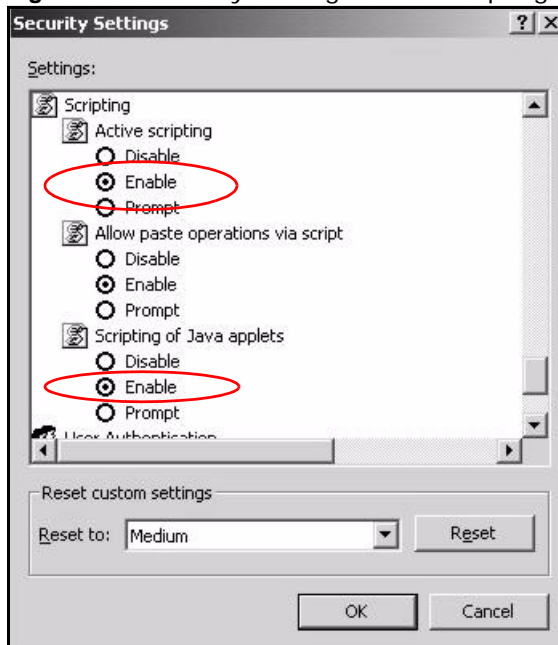
**Figure 194** Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

**Figure 195** Security Settings - Java Scripting

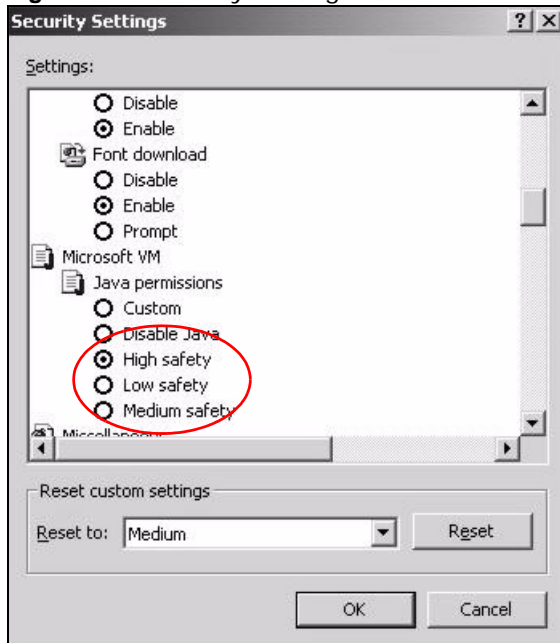


## Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

**Figure 196** Security Settings - Java

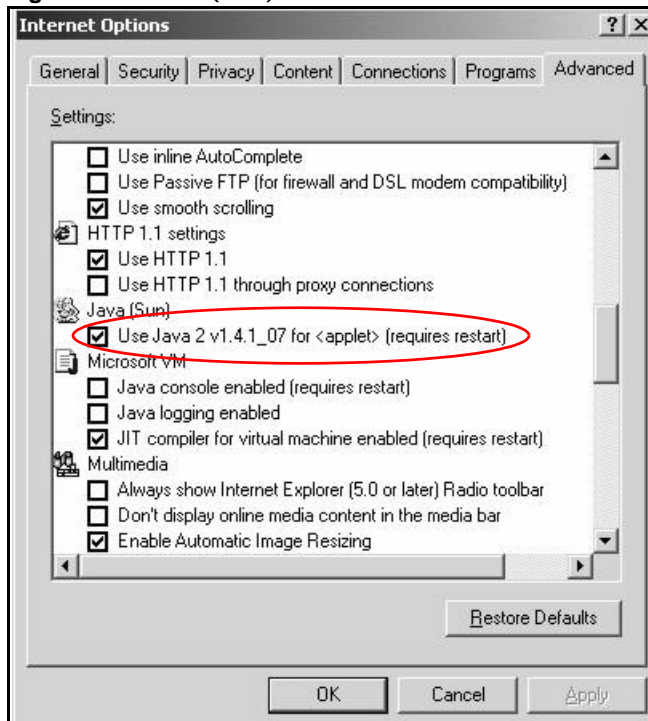


## JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

- 3 Click **OK** to close the window.

**Figure 197** Java (Sun)

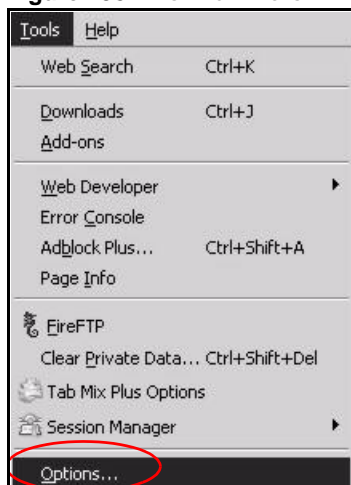


## Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

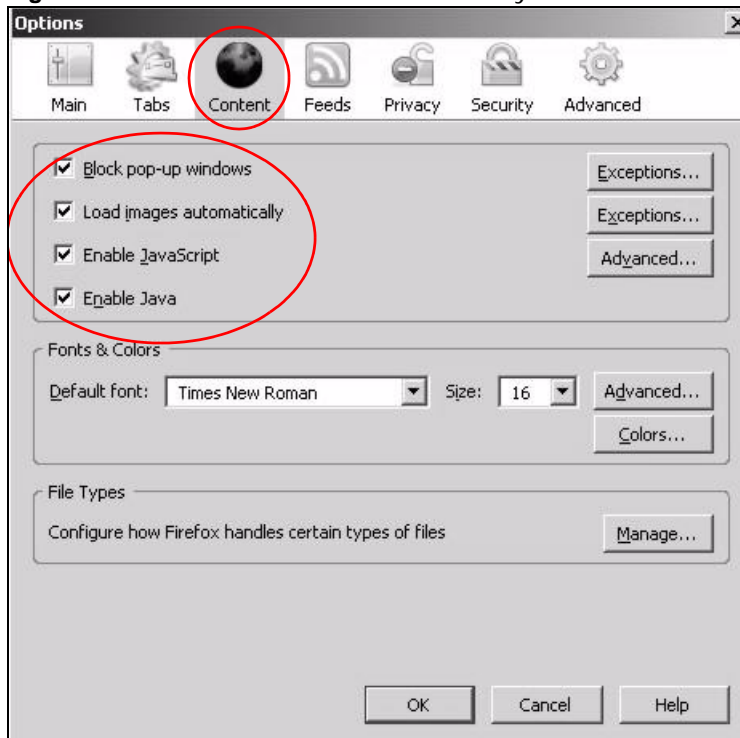
You can enable Java, JavaScript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

**Figure 198** Mozilla Firefox: Tools > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

**Figure 199** Mozilla Firefox Content Security





# Wireless LANs

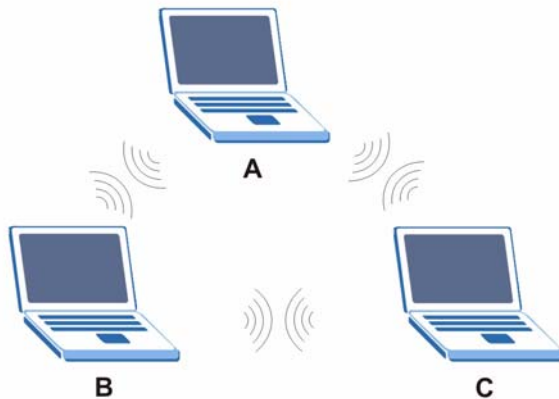
## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

**Figure 200** Peer-to-Peer Communication in an Ad-hoc Network



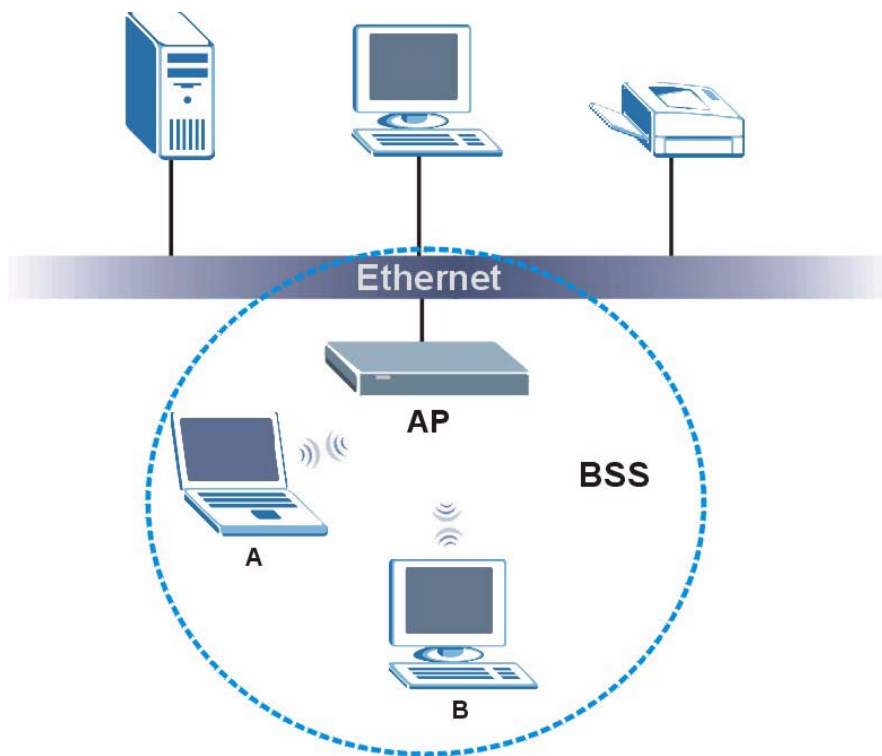
## BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is

disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

**Figure 201** Basic Service Set



## ESS

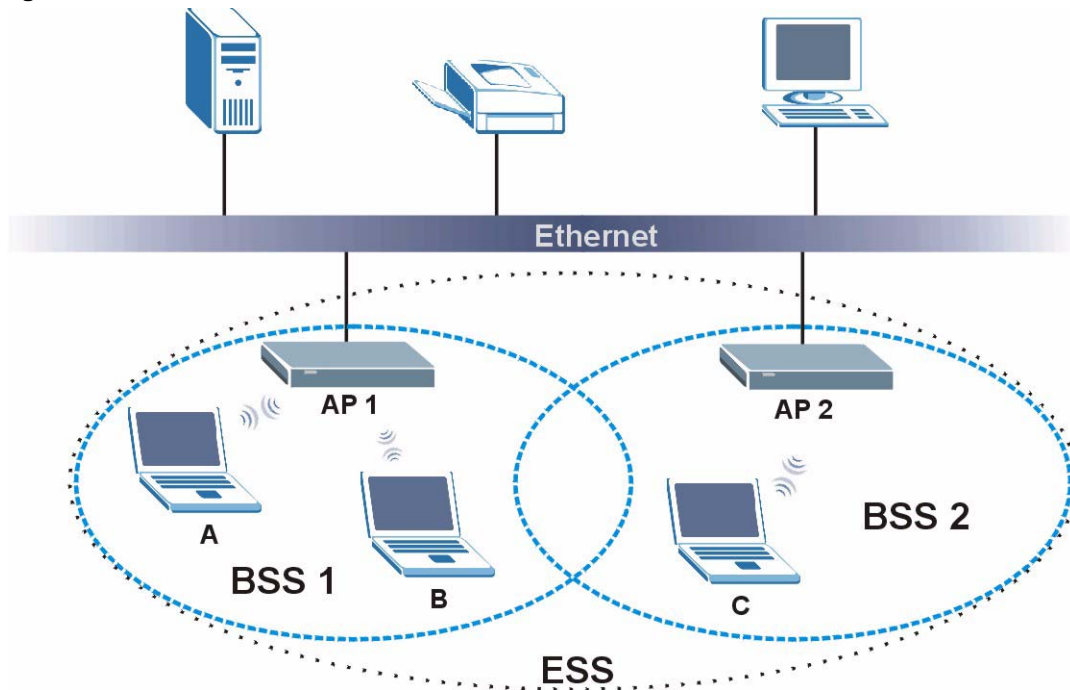
An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.



An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

**Figure 202** Infrastructure WLAN



## Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

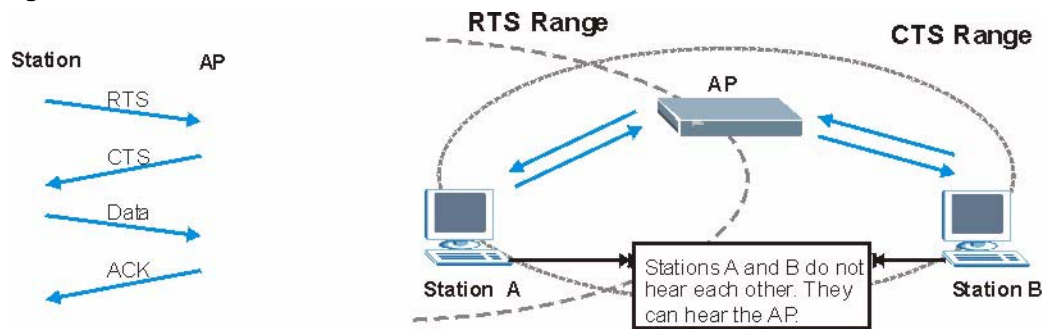
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they

cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 203** RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the Device uses long preamble.

Note: The wireless devices **MUST** use the same preamble mode in order to communicate.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 105** IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

## Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Device.

**Table 106** Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the Device and on all wireless clients that you want to associate with it.

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication  
Determines the identity of the users.
- Authorization  
Determines the network services available to authenticated users once they are connected to the network.
- Accounting  
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

## Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request  
Sent by an access point requesting authentication.
- Access-Reject  
Sent by a RADIUS server rejecting access.
- Access-Accept  
Sent by a RADIUS server allowing access.
- Access-Challenge  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request  
Sent by the access point requesting accounting.
- Accounting-Response  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

## Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

## EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

## EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

## EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

## PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

## LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

## Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

**Note:** EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 107** Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

## WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm

called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevents all wireless devices sharing the same encryption keys. (a weakness of WEP)

## User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go through the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

## Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

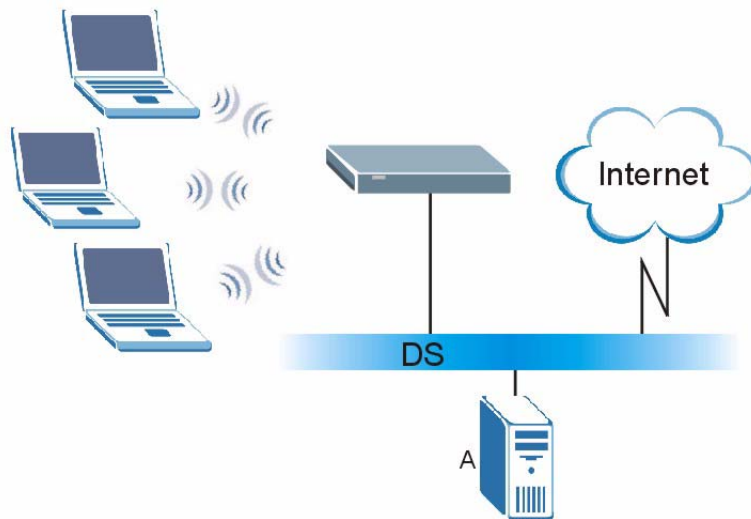


## WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 204** WPA(2) with RADIUS Application Example



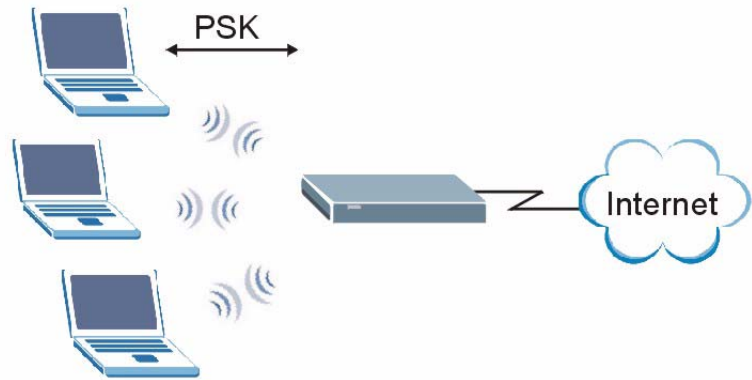
## WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

**Figure 205** WPA(2)-PSK Authentication



### Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 108** Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

### Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

## Antenna Characteristics

### Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

### Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

### Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

## Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

## Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

## WiFi Protected Setup

Your Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

### Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Device, see [Section 6.4 on page 133](#)).
- 3 Press the button on one of the devices (it doesn't matter which).
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

### PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (you can change it to a new random number by clicking on a button in the configuration interface).

When you use the PIN method, you must enter the enrollee's PIN into the registrar. Then, when WPS is activated on the enrollee, it presents its PIN to the registrar. If the PIN matches, the registrar sends the network and security information to the enrollee, allowing it to join the network.

The advantage of using the PIN method rather than the PBC method is that you can ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in the area. However, you need to log into the configuration interfaces of both devices.

Take the following steps to set up WPS using the PIN method.

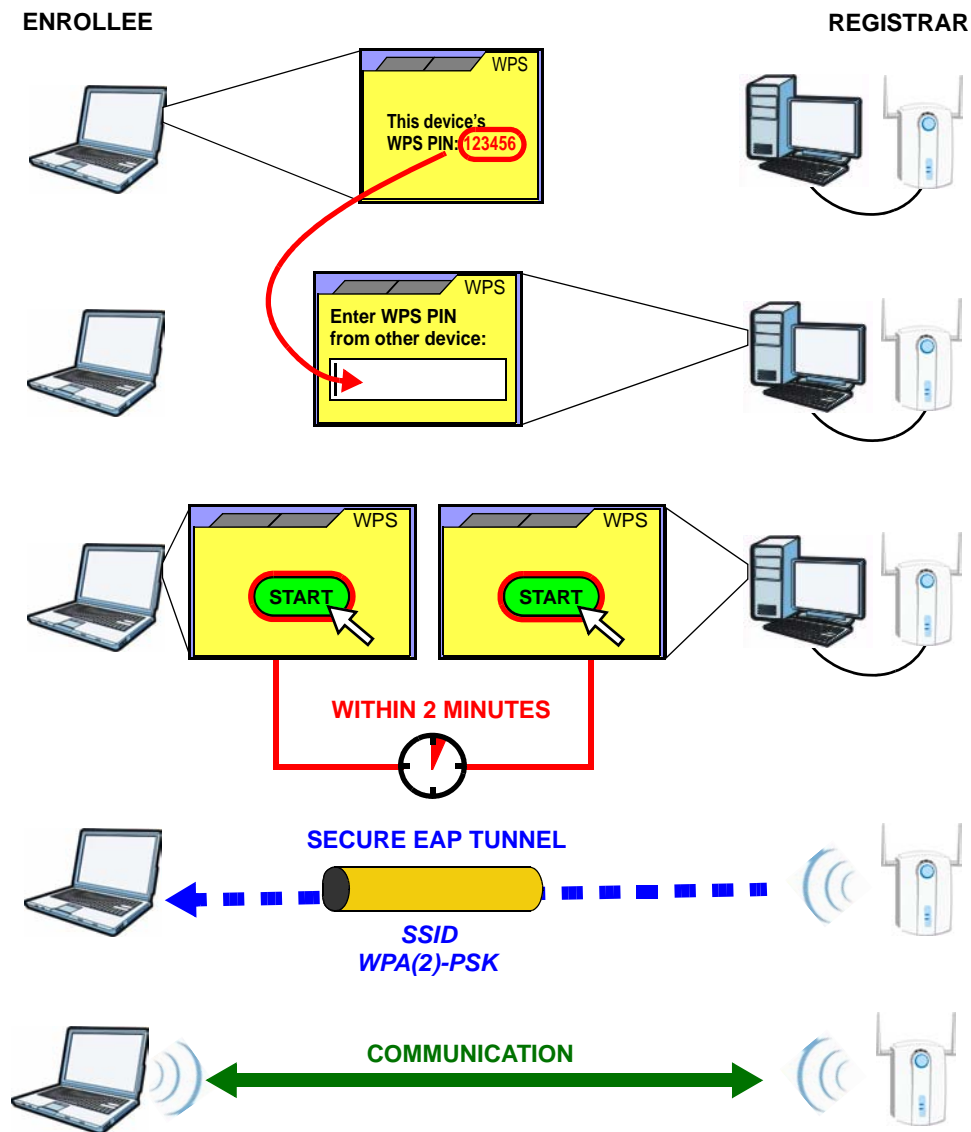
- 1 Decide which device you want to be the registrar (usually the AP) and which you want to be the enrollee (usually the client).
- 2 Look for the enrollee's WPS PIN; it may be displayed on the device. If you don't see it, log into the enrollee's configuration interface and locate the PIN. Select the PIN connection mode (not PBC connection mode). See the device's User's Guide for how to do this - for the Device, see [Section 6.4 on page 133](#).
- 3 Log into the configuration utility of the registrar. Select the PIN connection mode (not the PBC connection mode). Locate the place where you can enter the enrollee's PIN (if you are using the Device, see [Section 6.4 on page 133](#)). Enter the PIN from the enrollee device.
- 4 Activate WPS on both devices within two minutes.

Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

- 5 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.  
If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

**Figure 206** Example WPS Process: PIN Method

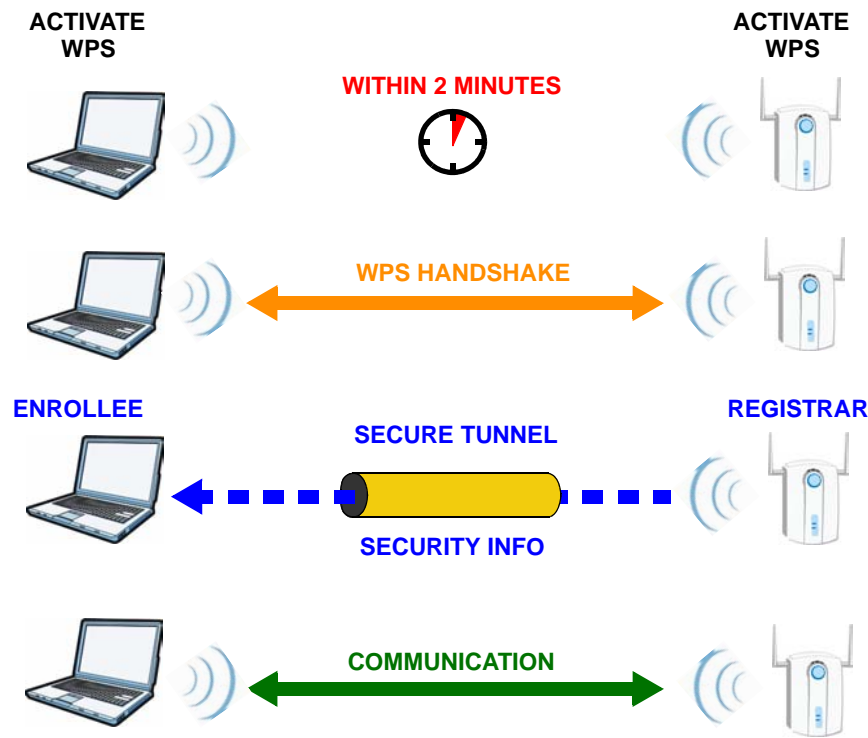


## How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

**Figure 207** How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS device is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

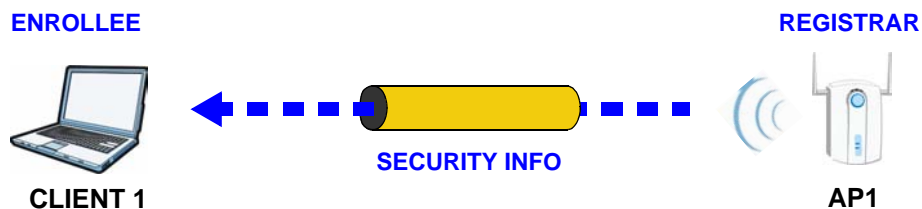
## Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1**

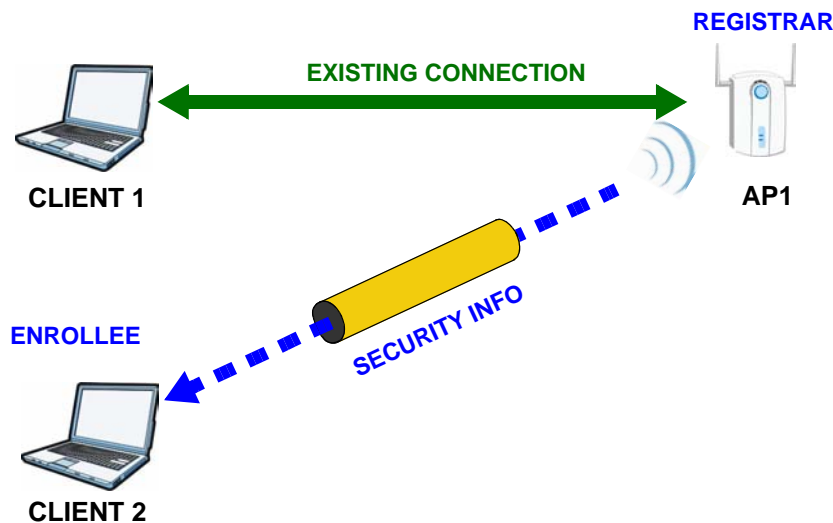
is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

**Figure 208** WPS: Example Network Step 1



In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

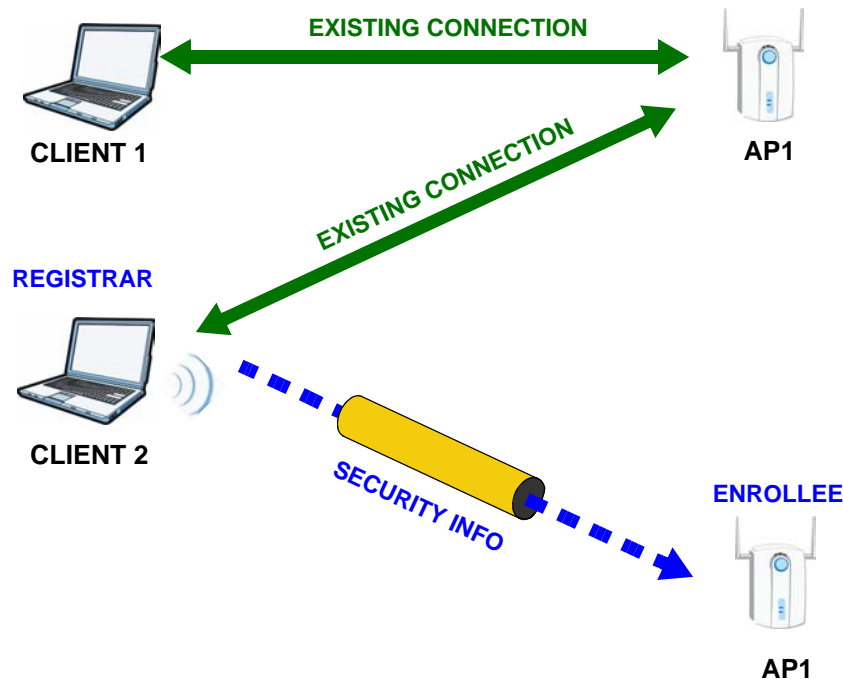
**Figure 209** WPS: Example Network Step 2





In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

**Figure 210** WPS: Example Network Step 3



## Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously; you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

## Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 109** Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

**Table 109** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.

**Table 109** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC: 1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.



## Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to  $3.4 \times 10^{38}$  IP addresses.

## IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address

2001:0db8:1a2b:0015:0000:0000:1a2f:0000.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So  
2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as  
2001:db8:1a2b:15:0:0:1a2f:0.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So  
2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as  
2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015,  
2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.

## Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

2001:db8:1a2b:15::1a2f:0/32

means that the first 32 bits (2001:db8) is the subnet prefix.

## Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

**Table 110** Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

## Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

## Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

## Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

## Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

**Table 111** Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.



The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

**Table 112** Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

## Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

## Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

## EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the

MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

MAC	00 : 13 : 49 : 12 : 34 : 56
EUI-64	02 : 13 : 49 : FF : FE : 12 : 34 : 56

## Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see [Interface ID](#) and [EUI-64](#)) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Device is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates <sup>5</sup>another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

## DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique Identifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

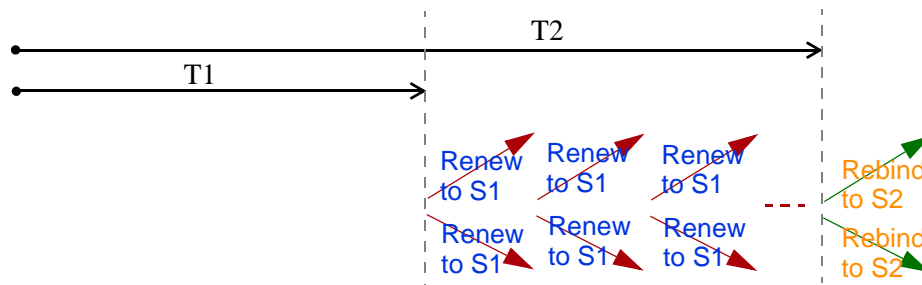
## Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the

---

5. In IPv6, all network interfaces can be associated with several addresses.

IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information. The IA type is the type of address in the IA. Each IA holds one type of address. IA\_NA means an identity association for non-temporary addresses and IA\_TA is an identity association for temporary addresses. An IA\_NA option contains the T1 and T2 fields, but an IA\_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA\_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA\_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA\_TA, the client may send a Renew or Rebind message at the client's discretion.



## DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

## Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

## ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

## Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

## IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Device also sends out a neighbor solicitation message. When the Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Device creates an entry in the default router list cache if the router can be used as a default router.

When the Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Device uses the prefix list to determine whether the destination address is on-link

and can be reached directly without passing through a router. If the address is unlinked, the address is considered as the next hop. Otherwise, the Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

## Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

### MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

## Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This

also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 10.1.1.46
    Subnet Mask . . . . .             : 255.255.255.0
    IP Address. . . . .               : fe80::2d0:59ff:feb8:103c%4
    Default Gateway . . . . .         : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

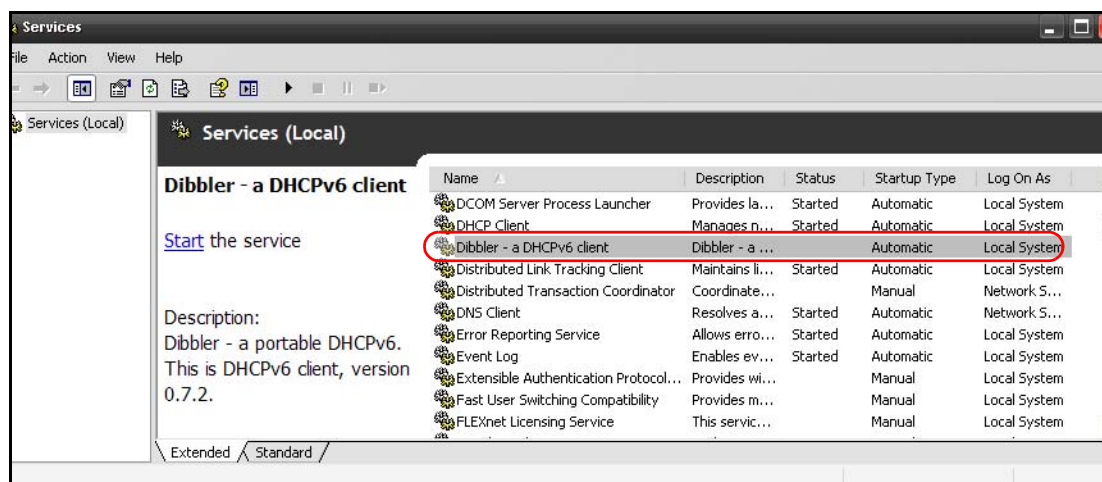
## Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

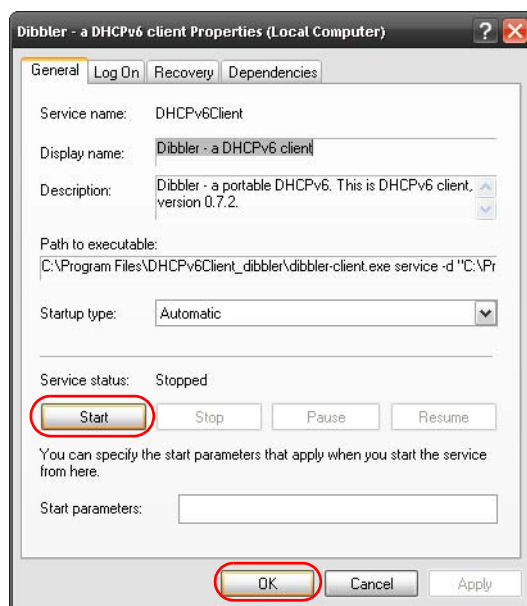
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

- 1 Install Dibbler and select the DHCPv6 client option on your computer.
- 2 After the installation is complete, select **Start > All Programs > Dibbler-DHCPv6 > Client Install as service.**
- 3 Select **Start > Control Panel > Administrative Tools > Services.**

- 4 Double click **Dibbler - a DHCPv6 client**.



- 5 Click **Start** and then **OK**.



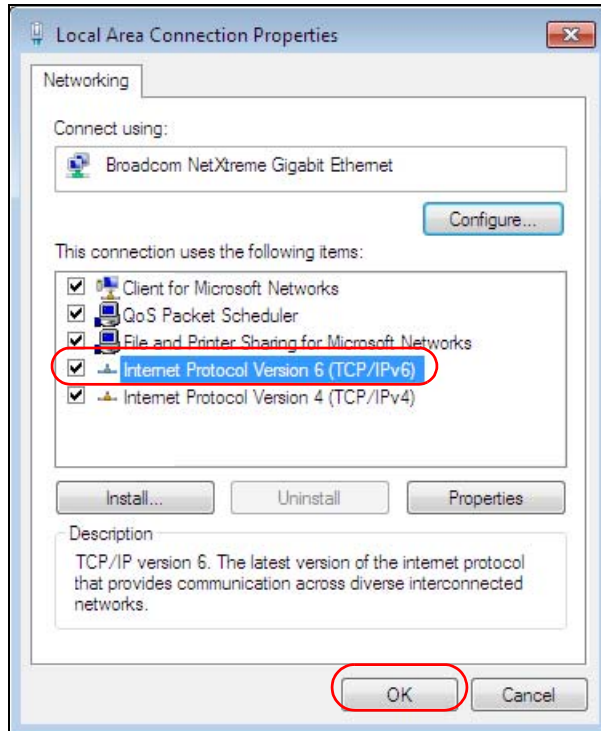
- 6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

## Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.



- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
```



# Open Software Announcements

## End-User License Agreement for “P-2812HNUL-Fx”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN-IN PART-SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS"). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTRIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

### 1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

### 2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

### 3. Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

#### 4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

#### 5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

#### 6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF

THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

#### 7.Limitation of Liability

IN NO EVENT WILL ZyxEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyxEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyxEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

#### 8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyxEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

#### 9.Audit Rights

ZyxEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

#### 10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyxEL all copies of the Software and Documentation in your possession or under your control. ZyxEL may terminate this License Agreement for any reason, including, but not limited to, if ZyxEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyxEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

#### 11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyxEL. Any waiver or modification of this License

Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

#### Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Bridge-utils, br2684ctl, Busybox, Dnsmasq, Ebttables, gettext, Igmpproxy, Iproute2, Iptables, libmccrypt, linux-atm, linuxigd, logrotate, MIPS linux kernel, Mtd-utils, P910nd, Ppp, Samba, Syslog-ng, Sysstat, Updatedd, usb-modeswitch, Usbmount, Wireless\_tools, and ntpclient under below GPL license

#### GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License

applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

#### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the



operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and

"any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes Dropbear and ncurses under the MIT License.

#### The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This Product includes eventlog, libedit, libupnp, Openssh, Ppp, Pure-ftpd, libpcap, and tcpdump under the license by BSD

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes wide-dhcpv6 under the following license

\$KAME: COPYRIGHT,v 1.2 2004/07/29 19:02:18 jinmei Exp \$

Copyright (C) 1998-2004 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Mini\_httpd under the license by ACME Labs Freeware

#### ACME Labs Freeware License

All the free software available on the ACME Labs web site has a copyright notice like this one:

Copyright © 2000 by Jef Poskanzer <jef@mail.acme.com>. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND

ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY

This Product includes glib, libbase64, libiconv, libusb, and mhash under the LGPL License.

## GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know

that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

#### GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has



appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-

compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended

to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes Flex under the following License.

Flex carries the copyright used for BSD software, slightly modified because it originated at the Lawrence Berkeley (not Livermore!) Laboratory, which operates under a contract with the Department of Energy:

Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007 The Flex Project.

Copyright (c) 1990, 1997 The Regents of the University of California.

All rights reserved.

This code is derived from software contributed to Berkeley by Vern Paxson.

The United States Government has rights in this work pursuant to contract no. DE-AC03-76SF00098 between the United States Department of Energy and the University of California.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This basically says "do whatever you please with this software except remove this notice or take advantage of the University's (or the flex authors') name".

Note that the "flex.skl" scanner skeleton carries no copyright notice. You are free to do whatever you please with scanners generated using flex; for them, you are not even bound by the above copyright.

This Product includes OpenSSL under the OpenSSL License.

#### LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

## OpenSSL License

-----

/\*

=====

\* Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

\*

\* Redistribution and use in source and binary forms, with or without

\* modification, are permitted provided that the following conditions

\* are met:

\*

\* 1. Redistributions of source code must retain the above copyright

\* notice, this list of conditions and the following disclaimer.

\*

\* 2. Redistributions in binary form must reproduce the above copyright

\* notice, this list of conditions and the following disclaimer in

\* the documentation and/or other materials provided with the

\* distribution.

\*

\* 3. All advertising materials mentioning features or use of this

\* software must display the following acknowledgment:

\* "This product includes software developed by the OpenSSL Project

\* for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

\*

\* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to

\* endorse or promote products derived from this software without

\* prior written permission. For written permission, please contact

\* [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

\*  
 \* 5. Products derived from this software may not be called "OpenSSL"  
 \* nor may "OpenSSL" appear in their names without prior written  
 \* permission of the OpenSSL Project.  
 \*  
 \* 6. Redistributions of any form whatsoever must retain the following  
 \* acknowledgment:  
 \* "This product includes software developed by the OpenSSL Project  
 \* for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"  
 \*  
 \* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY  
 \* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE  
 \* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR  
 \* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR  
 \* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,  
 \* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT  
 \* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;  
 \* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  
 \* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,  
 \* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)  
 \* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED  
 \* OF THE POSSIBILITY OF SUCH DAMAGE.  
 \*  
 \*  
 \*  
 \* This product includes cryptographic software written by Eric Young  
 \* (eay@cryptsoft.com). This product includes software written by Tim  
 \* Hudson (tjh@cryptsoft.com).

\*

\*/

Original SSLeay License

-----

/\* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

\* All rights reserved.

\*

\* This package is an SSL implementation written

\* by Eric Young (eay@cryptsoft.com).

\* The implementation was written so as to conform with Netscapes SSL.

\*

\* This library is free for commercial and non-commercial use as long as

\* the following conditions are aheared to. The following conditions

\* apply to all code found in this distribution, be it the RC4, RSA,

\* lhash, DES, etc., code; not just the SSL code. The SSL documentation

\* included with this distribution is covered by the same copyright terms

\* except that the holder is Tim Hudson (tjh@cryptsoft.com).

\*

\* Copyright remains Eric Young's, and as such any Copyright notices in

\* the code are not to be removed.

\* If this package is used in a product, Eric Young should be given attribution

\* as the author of the parts of the library used.

\* This can be in the form of a textual message at program startup or

\* in documentation (online or textual) provided with the package.

\*

\* Redistribution and use in source and binary forms, with or without



- \* modification, are permitted provided that the following conditions
- \* are met:
- \* 1. Redistributions of source code must retain the copyright
- \* notice, this list of conditions and the following disclaimer.
- \* 2. Redistributions in binary form must reproduce the above copyright
- \* notice, this list of conditions and the following disclaimer in the
- \* documentation and/or other materials provided with the distribution.
- \* 3. All advertising materials mentioning features or use of this software
- \* must display the following acknowledgement:
- \* "This product includes cryptographic software written by
- \* Eric Young (eay@cryptsoft.com)"
- \* The word 'cryptographic' can be left out if the routines from the library
- \* being used are not cryptographic related :-).
- \* 4. If you include any Windows specific code (or a derivative thereof) from
- \* the apps directory (application code) you must include an acknowledgement:
- \* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
- \*
- \* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
- \* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
- \* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
- \* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
- \* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
- \* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
- \* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
- \* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
- \* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
- \* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
- \* SUCH DAMAGE.

\*  
\* The licence and distribution terms for any publically available version or  
\* derivative of this code cannot be changed. i.e. this code cannot simply be  
\* copied and put under another distribution licence  
\* [including the GNU Public Licence.]  
\*/

This Product includes radvd under the following License

The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.
1. All terms of all other applicable copyrights and licenses must be followed.
2. Redistributions of source code must retain the authors' copyright notice(s), this list of conditions, and the following disclaimer.
3. Redistributions in binary form must reproduce the authors' copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. All advertising materials mentioning features or use of this software must display the following acknowledgement with the name(s) of the authors as specified in the copyright notice(s) substituted where indicated:

This product includes software developed by the authors which are mentioned at the start of the source files and other contributors.

5. Neither the name(s) of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ITS AUTHORS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes mcrypt under GPL V3 License

#### GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

#### Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

## TERMS AND CONDITIONS

### 0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

#### 1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

## 2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

## 3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

## 4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

## 5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

"a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

"b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

"c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

"d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

## 6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

"a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

"b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

"c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

"d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

"e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

## 7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.



Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

"a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

"b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

"c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

"d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

"e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

"f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

## 8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not

permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

#### 9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

#### 10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

#### 11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License,

through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

## 12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

## 13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

## 14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have

the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

#### 15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

#### 16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### 17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

#### How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <<http://www.gnu.org/licenses/>>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <<http://www.gnu.org/licenses/>>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <<http://www.gnu.org/philosophy/why-not-lgpl.html>>.

This Product includes popt under the following License

Copyright (c) 1998 Red Hat Software

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the X Consortium shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the X Consortium.

# Legal Information

## Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the Device is subject to the terms and conditions of any related service providers. Use with products that have NAT, and/or 3G.

Do not use the Device for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws, and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature. Use for products that have a download service.

Make sure all data and programs on the Device are also stored elsewhere. ZyXEL is not responsible for any loss of or damage to any data, programs, or storage media resulting from the use, misuse, or disuse of this or any other ZyXEL product. Use for storage/backup devices.

## Trademarks

This item incorporates copy protection technology that is protected by U.S. patents and other intellectual property rights of Rovi Corporation. Reverse engineering and disassembly are prohibited. Use for STBs that need Rovi certification.

## Certifications (Class B)

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.



### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 802.11g or 802.11n(20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n(40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

## 注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用  
者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現  
有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。  
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍  
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。  
減少電磁波影響，請妥適使用。



## Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

## Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

## **Registration**

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com).

# Index

## A

AAL5 [312](#)  
 ACK message [250](#)  
 activation  
     media server [162](#)  
     SSID [132](#)  
     wireless LAN  
         scheduling [137](#)  
 adding a printer example [66](#)  
 administrator password [30](#)  
 ADSL2 [312](#)  
 Advanced Encryption Standard, see AES  
 AES [383](#)  
 ALG [316](#)  
 alternative subnet mask notation [324](#)  
 antenna [309](#)  
     directional [388](#)  
     gain [387](#)  
     omni-directional [388](#)  
 AP (Access Point) [375](#)  
 Application Layer Gateway [316](#)  
 applications  
     Internet access [22](#)  
     media server [161](#)  
         activation [162](#)  
         iTunes server [161](#)  
     VoIP [23](#)  
 Asynchronous Transfer Mode [297](#)  
 ATM Adaptation Layer 5, see AAL5  
 audience [3](#)  
 authentication [138, 140](#)  
     RADIUS server [140](#)  
 auto dial [314](#)  
 automatic logout [30](#)  
 auto-negotiating rate adaptation [312](#)

## B

backup  
     configuration [291](#)  
 bandwidth management [187](#)  
 Basic Service Set, see BSS  
 blinking LEDs [26](#)  
 Broadband [93](#)  
 broadcast [117](#)  
 BSS [141, 373](#)  
     example [142](#)  
 BYE request [250](#)

## C

CA [219, 381](#)  
 call forwarding [315](#)  
 call hold [254](#)  
 call park and pickup [314](#)  
 call return [314](#)  
 call rule [243](#)  
 call service mode [253](#)  
 call transfer [254](#)  
 call waiting [254, 314](#)  
 caller ID [315](#)  
 Canonical Format Indicator See CFI  
 CBR (Constant Bit Rate) [100, 105, 108](#)  
 certificate  
     factory default [223](#)  
 Certificate Authority, see CA  
 certificates [219](#)  
     CA [219](#)  
     replacing [223](#)  
     storage space [223](#)  
     thumbprint algorithms [222](#)  
     thumbprints [222](#)  
     trusted CAs [224, 225](#)  
     verifying fingerprints [221](#)  
 Certification Authority, see CA

- certifications [425](#)
  - notices [425](#)
  - viewing [426](#)
- CFI [117](#)
- channel [375](#)
  - interference [375](#)
- channel scan [125](#)
- channel, wireless LAN [123](#)
- Class of Service [251](#)
- Class of Service, see CoS
- client list [156](#)
- client-server protocol [247](#)
- codecs [316](#)
- comfort noise generation [228](#), [315](#)
- command interface [25](#)
- configuration [164](#)
  - backup [291](#)
  - reset [293](#)
  - restoring [292](#)
- copyright [425](#)
- CoS [198](#), [251](#)
- country code [314](#)
- CTS (Clear to Send) [376](#)
- CTS threshold [138](#)

## D

- data fragment threshold [138](#)
- default LAN IP address [29](#)
- Denial of Service, see DoS
- device management
  - command interface [25](#)
  - Telnet [25](#)
- DHCP [90](#), [152](#), [164](#), [165](#), [209](#)
- DHCP relay [310](#)
- DHCP server [310](#)
- diagnostic [295](#)
- differentiated services [252](#)
- Differentiated Services, see DiffServ
- DiffServ (Differentiated Services) [251](#)
  - code points [251](#)
  - marking rule [199](#), [252](#)
- disclaimer [425](#)

- DLNA [161](#)
- DnD [314](#)
- DNS [152](#), [183](#)
- DNS server address assignment [117](#)
- Do not Disturb, see DnD
- domain name system, see DNS
- Domain Name System. See DNS.
- DS (Differentiated Services) [198](#)
- DS field [198](#), [252](#)
- DSCP [198](#), [251](#)
- DSL line, reinitialize [298](#)
- DTMF [251](#)
  - detection and generation [316](#)
- Dual-Tone MultiFrequency, see DTMF
- dynamic DNS [209](#)
- Dynamic Host Configuration Protocol, see DHCP
- dynamic jitter buffer [315](#)
- dynamic WEP key exchange [382](#)
- DYNDNS wildcard [209](#)

## E

- EAP Authentication [380](#)
- echo cancellation [229](#), [315](#)
- Encapsulation [113](#)
  - MER [113](#)
  - PPP over Ethernet [113](#)
- encapsulation [95](#)
  - RFC 1483 [113](#)
- encryption [140](#), [383](#)
- ESS [374](#)
- Europe type call service mode [253](#)
- Extended Service Set IDentification [124](#), [133](#)
- Extended Service Set, see ESS
- external antenna [316](#)
- external RADIUS [317](#)

## F

- F4/F5 OAM [312](#)
- File Sharing [159](#)
- file sharing [24](#)

- filters
  - MAC address [139](#)
- firewalls [211](#)
  - configuration [213](#)
  - security [215](#)
- firmware [289](#)
- flash key [253](#)
- flashing [253](#)
- fragmentation threshold [138](#), [377](#)
- frequency range [317](#)
- FTP [202](#)

## G

- G.168 [229](#), [315](#)
- G.711 [316](#)
- G.729 [316](#)
- G.992.1 [312](#)
- G.992.3 [312](#)
- G.992.5 [312](#)

## H

- hidden node [375](#)
- host [265](#)
- host name [89](#)
- humidity [309](#)

## I

- IAD [21](#)
- IANA [166](#), [330](#)
- IBSS [373](#)
- IEEE 802.11g [377](#)
- IEEE 802.11g wireless LAN [316](#)
- IEEE 802.11i [316](#)
- IEEE 802.1Q [116](#)
- IEEE 802.1Q VLAN [252](#)
- IGMP [117](#)
  - version [117](#)

- IGMP proxy [313](#)
- IGMP v1 [313](#)
- IGMP v2 [313](#)
- importing trusted CAs [225](#)
- Independent Basic Service Set, see IBSS
- initialization vector (IV) [383](#)
- install UPnP [168](#)
  - Windows Me [168](#)
  - Windows XP [170](#)
- Integrated Access Device, see IAD
- intended audience [3](#)
- Internet access [22](#)
- Internet Assigned Numbers Authority
  - See IANA
- Internet Assigned Numbers Authority, see IANA
- Internet Service Provider, see ISP
- IP address [90](#), [165](#)
  - default [29](#)
  - ping [295](#)
  - WAN [95](#)
- IP Address Assignment [116](#)
- IP multicasting [313](#)
- IP pool [156](#)
- IP pool setup [165](#)
- ISP [95](#)
- iTunes server [161](#)
- ITU-T [229](#)
- ITU-T G.992.1 [298](#)

## J

- jitter buffer [315](#)

## L

- LAN [151](#)
  - and USB printer [163](#)
  - client list [156](#)
  - MAC address [157](#)
- LAN TCP/IP [165](#)
- limitations
  - wireless LAN [141](#)

- WPS [148](#)
- listening port [232](#)
- Local Area Network, see LAN
- login
  - passwords [30](#)
- logout [30](#)
  - automatic [30](#)
- logs [257](#), [261](#), [277](#)

## M

- MAC [89](#), [217](#)
- MAC address [157](#)
  - filter [139](#)
- MAC address filtering [217](#)
- MAC filter [217](#)
- managing the device
  - command interface [25](#)
  - good habits [26](#)
  - Telnet [25](#)
  - using FTP. See FTP.
- Maximum Burst Size (MBS) [100](#), [105](#), [109](#), [114](#)
- MBSSID [142](#)
- Media access control [217](#)
- Media Access Control, see MAC Address
- media server [161](#)
  - activation [162](#)
  - iTunes server [161](#)
- Message Integrity Check, see MIC
- MIC [383](#)
- model name [89](#)
- MTU (Multi-Tenant Unit) [116](#)
- multicast [117](#)
- multimedia [245](#)
- Multiple BSS, see MBSSID
- multiple PVC support [311](#)
- multiple SIP accounts [315](#)
- multiple voice channels [315](#)
- multiplexing [114](#)
  - LLC-based [114](#)
  - VC-based [114](#)
- multiprotocol encapsulation [113](#)

## N

- NAT [165](#), [203](#), [329](#)
  - definitions [206](#)
  - how it works [207](#)
  - what it does [207](#)
- Network Address Translation, see NAT
- network map [33](#)
- non-proxy calls [243](#)

## O

- OAM [312](#)
- OK response [250](#)
- operation humidity [309](#)
- operation temperature [309](#)

## P

- Pairwise Master Key (PMK) [383](#), [385](#)
- park [314](#)
- passphrase [127](#)
- passwords [30](#)
- PBC [143](#)
- Peak Cell Rate (PCR) [100](#), [105](#), [108](#), [114](#)
- peer-to-peer calls [243](#)
- Per-Hop Behavior, see PHB
- PHB [199](#), [252](#)
- phone book
  - speed dial [243](#)
- phone config [314](#)
- pickup [314](#)
- PIN, WPS [144](#)
  - example [145](#)
- point-to-point calls [316](#)
- ports [26](#)
- power adaptor [317](#)
- power specifications [309](#)
- PPP (Point-to-Point Protocol) Link Layer Protocol [313](#)
- PPP over ATM AAL5 [312](#)
- PPP over Ethernet [312](#)

PPP over Ethernet, see PPPoE  
 PPPoE [95](#), [113](#), [311](#)  
     Benefits [113](#)  
 preamble [138](#)  
 preamble mode [377](#)  
 print server [24](#)  
 Printer Server [163](#)  
 printer sharing  
     and LAN [163](#)  
     configuration [61](#)  
     requirements [163](#)  
     TCP/IP port [61](#)  
 product registration [426](#)  
 profile [45](#)  
 protocol [95](#)  
 PSK [383](#)  
 PSTN call setup signaling [251](#)  
 pulse dialing [251](#)  
 Push Button Configuration, see PBC  
 push button, WPS [143](#)

## Q

QoS [187](#), [188](#), [198](#), [251](#), [315](#)  
 Quality of Service [315](#)  
 Quality of Service, see QoS  
 quick dialing [316](#)  
 Quick Start Guide [29](#)

## R

RADIUS [317](#), [379](#)  
     message types [379](#)  
     messages [379](#)  
     shared secret key [380](#)  
 RADIUS server [140](#)  
 Reach-Extended ADSL [312](#)  
 Real time Transport Protocol, see RTP  
 region [314](#)  
 registration  
     product [426](#)  
 reinitialize the ADSL line [298](#)

related documentation [3](#)  
 REN [315](#)  
 Request To Send, see RTS  
 reset [293](#)  
 RESET button [28](#)  
 restart [293](#)  
 restoring configuration [292](#)  
 RFC 1483 [113](#), [312](#)  
 RFC 1631 [201](#)  
 RFC 1889 [249](#), [316](#)  
 RFC 1890 [316](#)  
 RFC 2327 [316](#)  
 RFC 2364 [312](#)  
 RFC 2516 [311](#), [312](#)  
 RFC 2684 [312](#)  
 RFC 3261 [316](#)  
 Ringer Equivalence Number, see REN  
 router features [22](#)  
 RTCP [316](#)  
 RTP [249](#), [316](#)  
 RTS (Request To Send) [376](#)  
     threshold [375](#), [376](#)  
 RTS threshold [138](#)

## S

safety warnings [7](#)  
 scan [125](#)  
 scheduling  
     wireless LAN [137](#)  
 SDP [316](#)  
 seamless rate adaptation [312](#)  
 security  
     wireless LAN [138](#)  
 security, network [215](#)  
 service access control [270](#)  
 Service Set [124](#), [133](#)  
 Session Description Protocol [316](#)  
 Session Initiation Protocol, see SIP  
 silence suppression [228](#), [315](#)  
 SIP [245](#)  
     account [245](#)  
     accounts [315](#)

- ALG [316](#)
- Application Layer Gateway [316](#)
- call progression [249](#)
- client [247](#)
- identities [245](#)
- INVITE request [250](#)
- number [246](#)
- proxy server [247](#)
- redirect server [248](#)
- register server [249](#)
- servers [247](#)
- service domain [246](#)
- URI [245](#)
- user agent [247](#)
- version 2 [316](#)
- SMTP error messages [278](#)
- SNMP [313](#)
- speed dial [243](#)
- SRA [312](#)
- SSID [139](#)
  - activation [132](#)
  - MBSSID [142](#)
- stateful inspection [311](#)
- static route [179](#)
- static VLAN
- status [87](#)
- status indicators [26](#)
- storage humidity [309](#)
- storage temperature [309](#)
- subnet [321](#)
- subnet mask [165](#), [322](#)
- subnetting [324](#)
- supplementary services [252](#)
- Sustain Cell Rate (SCR) [100](#), [105](#), [109](#)
- Sustained Cell Rate (SCR) [114](#)
- syntax conventions [5](#)
- system
  - firmware [289](#)
  - passwords [30](#)
  - status [87](#)
- System Info [89](#)
- system name [89](#), [272](#)

## T

- Tag Control Information See TCI
- Tag Protocol Identifier See TPID
- TCI
- TCP/IP port [61](#)
- Telnet [25](#)
- temperature [309](#)
- Temporal Key Integrity Protocol, see TKIP
- The [95](#)
- three-way conference [254](#)
- thresholds
  - data fragment [138](#)
  - RTS/CTS [138](#)
- TKIP [383](#)
- ToS [251](#)
- TPID [116](#)
- traffic shaping [114](#)
- transparent bridging [313](#)
- trusted CAs, and certificates [224](#)
- tutorial
  - VoIP [51](#)
  - wireless [40](#)
- Type of Service, see ToS

## U

- unicast [117](#)
- Uniform Resource Identifier [245](#)
- Universal Plug and Play, see UPnP
- upgrading firmware [289](#)
- UPnP [158](#)
  - forum [153](#)
  - security issues [153](#)
- USB features [24](#)
- USB printer [24](#)

## V

- VAD [228](#), [315](#)
- version
  - firmware



- version [90](#)
- VID
- Virtual Circuit (VC) [114](#)
- Virtual Local Area Network See VLAN
- Virtual Local Area Network, see VLAN
- VLAN [116, 252](#)
  - group [252](#)
  - ID [252](#)
  - ID tags [252](#)
  - Introduction [116](#)
  - number of possible VIDs
  - priority frame
  - static
- VLAN ID [116](#)
- VLAN Identifier See VID
- VLAN tag [116](#)
- voice activity detection [228, 315](#)
- voice channels [315](#)
- voice coding [250](#)
- VoIP [245](#)
  - features [23](#)
  - peer-to-peer calls [243](#)
  - standards compliance [315](#)
  - tutorial [51](#)
- VoIP features [23](#)

## W

- WAN
  - Wide Area Network, see WAN [93](#)
- warnings [7](#)
- warranty [426](#)
  - note [426](#)
- Web Configurator [29](#)
- web configurator
  - passwords [30](#)
- WEP [127, 141, 316](#)
- WEP Encryption [128](#)
- Wi-Fi Protected Access, see WPA
- Wired Equivalent Privacy, see WEP
- wireless
  - client configuration [42](#)
  - profile [45](#)
  - security [378](#)
  - tutorial [40](#)
  - wireless client WPA supplicants [384](#)
  - wireless LAN [121](#)
    - authentication [138, 140](#)
    - BSS [141](#)
      - example [142](#)
    - channel [123](#)
    - encryption [140](#)
    - example [122](#)
    - fragmentation threshold [138](#)
    - limitations [141](#)
    - MAC address filter [139, 316](#)
    - MBSSID [142](#)
    - preamble [138](#)
    - RADIUS server [140](#)
    - RTS/CTS threshold [138](#)
    - scheduling [137](#)
    - security [138](#)
    - SSID [139](#)
      - activation [132](#)
    - WEP [141](#)
    - WPA [141](#)
    - WPA-PSK [141](#)
    - WPS [143, 145](#)
      - example [147](#)
      - limitations [148](#)
      - PIN [144](#)
      - push button [143](#)
  - wireless network
    - example [121](#)
  - wireless security [378](#)
  - WLAN [121](#)
    - auto-scan channel [125](#)
    - interference [375](#)
    - passphrase [127](#)
    - scheduling [137](#)
    - security parameters [386](#)
    - see also wireless.
    - WEP [127](#)
  - WLAN button [25](#)
  - WPA [141, 316, 382](#)
    - key caching [384](#)
    - pre-authentication [384](#)
    - user authentication [384](#)
    - vs WPA-PSK [383](#)
    - wireless client supplicant [384](#)
    - with RADIUS application example [384](#)
  - WPA2 [382](#)

- user authentication [384](#)
- vs WPA2-PSK [383](#)
- wireless client supplicant [384](#)
- with RADIUS application example [384](#)
- WPA2-Pre-Shared Key, see WPA2-PSK
- WPA2-PSK [382](#), [383](#)
  - application example [385](#)
- WPA-PSK [141](#), [383](#)
  - application example [385](#)
- WPS [143](#), [145](#)
  - example [147](#)
  - limitations [148](#)
  - PIN [144](#)
    - example [145](#)
  - push button [143](#)